Quels droits sur les données ?

Knockaert, Manon; Tombal, Thomas

Published in:
Actualités en droit du numérique

Publication date:
2019

Document Version
le PDF de l'éditeur

Quels droits sur les données ?

Manon Knockaert
Chercheuse au CRIDS-NaDI UNamur

Thomas Tombal
Chercheur et doctorant au CRIDS-NaDI UNamur

Introduction

1. Les données sont souvent présentées comme étant le « pétrole de l'économie moderne »[1]. Certes, celles-ci ne servent pas de carburant pour faire fonctionner nos voitures ou nos chaudières, mais, en revanche, elles sont le carburant de la création d'informations et de connaissances dans un monde toujours plus connecté. Ainsi, les données sont « une ressource essentielle pour la croissance économique, la création d'emplois et le progrès sociétal »[2], et la valeur de l'économie fondée sur les données devrait avoisiner 643 milliards d'euros d'ici à 2020[3]. Un tel nombre ne surprend pas, tant la quantité de données générées augmente de façon exponentielle. Par ailleurs, cette augmentation n'est pas prête de s'arrêter, car l'émergence de l'« internet des objets »[4] vient contribuer à l'exacerbation de ce phénomène.

Comme la Commission européenne l'a souligné à juste titre dans sa communication intitulée « Créer une économie européenne fondée sur les données », sur laquelle nous reviendrons plus longuement *infra*[5] :

> « Des volumes toujours croissants de données sont produits par des machines ou des processus fondés sur des technologies émergentes, tels que l'internet des objets. Ces données constituent une composante de plus en plus importante

1 J. Drexl, « Designing Competitive Markets for Industrial Data – Between Propertisation and Access », *Max Planck Institute for Innovation & Competition Research Paper*, 31 octobre 2016, n° 16-13, p. 2, disponible sur https://ssrn.com/abstract=2862975. Traduction libre de : *The oil of the modern economy*.

2 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, « Créer une économie européenne fondée sur les données », Bruxelles, 10 janvier 2017, COM(2017) 9 final, p. 2.

3 *Ibid.*

4 « L'internet des objets, ou IdO (en anglais *Internet of Things*, ou IoT) est l'interconnexion entre internet et des objets, des lieux et des environnements physiques. L'appellation désigne un nombre croissant d'objets connectés à internet permettant ainsi une communication entre nos biens dits physiques et leurs existences numériques. Ces formes de connexions permettent de rassembler de nouvelles masses de données sur le réseau et donc, de nouvelles connaissances et formes de savoirs » (https://fr.wikipedia.org/wiki/Internet_des_objets).

5 Voy. *infra*, section 2.

> des nouveaux services innovants qui permettent d'améliorer les produits ou processus de production et de fournir une assistance à la prise de décision. »[6]

Dans cette communication, la Commission européenne qualifie ce type de données sous le vocable de « données produites par des machines », définies comme étant des données « générées sans intervention humaine directe, par des processus informatiques, des applications ou des services, ou par des capteurs qui traitent des informations reçues d'équipements, de logiciels ou de dispositifs virtuels ou réels »[7]. Citons ainsi, à titre d'exemple, les données (qui seront) générées par les véhicules autonomes, les maisons intelligentes, les engins agricoles intelligents, les bracelets connectés, etc.

2. Si la valeur économique dérivant du traitement de ces données paraît évidente, la détermination du cadre juridique devant être appliqué à celles-ci est, au contraire, une tâche complexe. Ainsi, comme le souligne la Commission européenne :

> « Des règles modernes et cohérentes dans l'ensemble de l'UE [s'imposent] pour que les données puissent circuler librement d'un État membre à l'autre [...] [et] l'absence d'environnement juridique adapté aux échanges de données dans l'UE [risque] de restreindre l'accès aux grands ensembles de données, de créer des barrières à l'entrée pour les nouveaux venus sur le marché et de freiner l'innovation. »[8]

La difficulté de l'élaboration d'un tel cadre juridique européen résulte du fait que les données sont un bien complexe, sur lequel de nombreuses personnes physiques ou morales peuvent potentiellement revendiquer un droit ou un intérêt. Ainsi, les données générées par un véhicule autonome sont pertinentes pour de multiples catégories d'acteurs, tels que les fabricants du véhicule, les concessionnaires, les fabricants de pièces détachées, les garagistes et réparateurs agréés et indépendants, les développeurs de logiciels utilisés dans les véhicules, les usagers du véhicule, une éventuelle société de leasing et même, dans certains cas, les autorités publiques si certaines de ces données peuvent s'avérer précieuses pour l'optimisation de la gestion du trafic routier. Cet exemple illustre la complexité inhérente à cette ressource, qui se trouvera bien souvent au croisement de multiples prétentions et droits, visant à contrôler, avoir accès à, ou tirer profit du traitement de ces données.

Ceci met en lumière la nécessité de l'élaboration d'un cadre juridique clair, d'autant plus que le marché des données n'en est qu'à ses balbutiements, puisque seul un nombre limité d'entreprises (6,3 %) prennent activement part dans l'échange de données entre entreprises[9].

6 Communication de la Commission, « Créer une économie européenne fondée sur les données », *op. cit.*, p. 9.

7 *Ibid.*, p. 10.

8 *Ibid.*, p. 3.

9 M. Barbero, D. Cocoru, H. Graux, A. Hillebrand, F. Linz, D. Osimo, A. Siede et P. Wauters, « Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability », 25 avril 2018, p. 31, disponible sur https://ec.europa.eu/digital-single-market/en/news/study-emerging-issues-data-ownership-interoperability-re-usability-and-access-data-and.

3. Compte tenu de ce contexte, l'objectif de cette contribution sera double. D'une part, celle-ci aura pour but de dresser un panorama du cadre juridique européen et belge actuel, applicable, directement ou indirectement, aux données (section 1). D'autre part, cette intervention mettra en lumière les initiatives de la Commission européenne dans le cadre de la création d'une « économie européenne fondée sur les données » (section 2).

Section 1
Panorama du cadre juridique actuel

4. Au vu de la nature complexe des données, une pléiade de textes juridiques européens et belges sont susceptibles de s'appliquer, directement ou indirectement, aux données. Ce faisant, cette section abordera, d'une part, les instruments juridiques conférant, directement ou indirectement, des droits sur les données (§ 1), et d'autre part, les instruments juridiques limitant les droits sur les données, favorisant ainsi leur circulation (§ 2).

§ 1. Instruments juridiques conférant des droits sur les données

5. Précisons d'emblée, en guise d'introduction, que les divers instruments étudiés ci-après ne sont pas exclusifs les uns des autres, mais peuvent très bien, dans certains cas, s'appliquer cumulativement à un même jeu de données.

A. Données à caractère personnel

6. Les données, produites notamment via l'internet des objets, peuvent tout d'abord être soumises au régime de protection des données à caractère personnel[10]. Ces dernières sont définies par le règlement général sur la protection des données[11] (ci-après « RGPD ») comme étant :

> « [...] toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant [...] »[12].

10 Pour de plus amples informations quant à ce régime de protection, voy., dans cet ouvrage, J.-F. Puyraimond, « La gestion des données personnelles par l'entreprise : dis-moi ce que tu traites et je te dirai comment faire (ou : de l'importance du registre des données) ».

11 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.*, L 119, 4 mai 2016. En droit belge, le RGPD est complété par la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018, et la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018.

12 Article 4, 1), du RGPD. Cette définition est raffinée par le considérant 26 du RGPD : « Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour

Citons à titre d'exemple les données de consommation collectées par un frigo intelligent, qui pourrait notamment révéler l'orientation religieuse d'une personne achetant des produits kasher ou halal. Pensons également à la géolocalisation de l'usager effectuée par un véhicule autonome ou une montre connectée.

7. Les règles relatives à la protection des données à caractère personnel, et plus particulièrement le RGPD, constituent un champ du droit de l'UE essentiel à prendre en compte au vu de cette définition large de ce que constitue une donnée à caractère personnel. De fait, bien souvent, il ne sera pas aisé de déterminer si une catégorie de données, produites par des machines ou non, devra être considérée comme personnelle ou non.

Par ailleurs, avec le développement constant des technologies d'analyse big data[13], cette difficulté risque de s'accentuer. En effet, le big data accroît la possibilité de « croiser » de multiples jeux de données, auxquels il était auparavant plus difficile d'avoir accès, ce qui exacerbe, en conséquence, le risque de réidentification directe ou indirecte d'une personne concernée sur base de ces données, que ce soit par le responsable de traitement[14] ou par un tiers. Ce faisant, des données considérées à un temps T comme étant non personnelles peuvent dès lors, en raison de l'évolution technologique des capacités d'analyse de données, devenir au temps T+1 des données à caractère personnel. Il convient donc de garder à l'esprit ce caractère évolutif de la définition de la nature personnelle ou non d'une donnée.

Ainsi, dès la fin des années 1990, un chercheur aux États-Unis a réussi à réidentifier plus de 80 % des personnes dont les données étaient contenues dans une base de données d'une entreprise privée active dans le secteur de la santé, alors pourtant que ces données étaient censées être anonymisées[15]. En réalité, si les noms de ces personnes avaient bien été effacés, la base de données contenait encore des informations d'ordre médical ainsi que le code postal, le sexe, et la date de naissance complète[16]. Or, ces trois dernières informations figuraient également dans les registres de listes électorales, accessibles au public, ce qui a permis à ce chercheur de croiser ces données, d'identifier 80 % des personnes contenues dans le fichier et de prendre ainsi connaissance

identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci. »

13 « Le *big data*, littéralement "grosses données", ou mégadonnées (recommandé), parfois appelées données massives, désigne des ensembles de données devenus si volumineux qu'ils dépassent l'intuition et les capacités humaines d'analyse et même celles des outils informatiques classiques de gestion de base de données ou de l'information » (https://fr.wikipedia.org/wiki/Big_data).

14 L'article 4, 7), du RGPD définit le responsable de traitement comme étant : « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ».

15 Groupe de travail « Article 29 », « Avis 05/2014 sur les Techniques d'anonymisation », WP 216, 10 avril 2014, p. 30, disponible sur www.dataprotection.ro/servlet/ViewDocument?id=1288.

16 *Ibid.*

de l'état de santé de ces personnes[17]. Cet exemple illustre bien le fait que le risque de réidentification augmente avec le développement des nouvelles technologies et l'accès croissant à de larges amas de données.

8. Précisons encore que des données à caractère personnel pseudonymisées, à savoir des données auxquelles un traitement a été appliqué de sorte que « celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable »[18], restent soumises au RGPD, car la personne concernée demeure réidentifiable par le biais de croisement de données[19]. Seules les données à caractère personnel ayant été anonymisées[20] échappent aux dispositions du RGPD, car elles ne permettent plus la réidentification des personnes concernées[21].

Ainsi, dans l'exemple utilisé au point précédent, les données n'avaient pas été anonymisées, mais uniquement pseudonymisées, car les personnes ont pu être réidentifiées en croisant la base de données avec des registres publics.

9. L'un des objectifs du RGPD est d'encadrer l'utilisation commerciale des données à caractère personnel, en rendant aux personnes concernées le contrôle sur « leurs » données. Ce contrôle se manifeste par l'octroi d'une série de droits aux personnes concernées[22], tels que le droit à l'information, le droit d'accès, le droit à la portabilité[23] ou encore le droit à l'effacement[24]. Ce souci du législateur européen, visant à rendre aux personnes concernées une forme de contrôle sur leurs données personnelles, s'inscrit dans la préoccupation plus large de la promotion du droit à l'autodétermination informationnelle de celles-ci, qui découle du droit à la dignité humaine[25].

Partant, le RGPD ne confère aucunement un quelconque droit de « propriété » sur les données à caractère personnel. De fait, bien que la pratique tende à

17 *Ibid.*

18 Article 4, 5), du RGPD.

19 Considérant 26 du RGPD.

20 La norme ISO 29100 définit l'anonymisation comme étant : « le processus par lequel des informations personnellement identifiables (IPI) sont irréversiblement altérées de telle façon que le sujet des IPI ne puisse plus être identifié directement ou indirectement, que ce soit par le responsable du traitement des IPI seul ou en collaboration avec une quelconque autre partie » (ISO 29100:2011).

21 Considérant 26 du RGPD.

22 Voy. le chapitre III du RGPD, articles 12 à 23. Pour une étude détaillée des différents droits de la personne concernée, voy. Th. Tombal, « Les droits de la personne concernée dans le RGPD », *in* C. de Terwangne et K. Rosier (coord.), *Le Règlement général sur la protection des données (RGPD/GDPR) – Analyse approfondie*, Bruxelles, Larcier, 2018, pp. 407-557.

23 Voy. *infra*, points 35 à 37.

24 Droit à l'information (articles 12 à 14) ; droit d'accès (article 15), droit à la portabilité (article 20) ; droit à l'effacement (article 17).

25 C. de Terwangne, « La réforme de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », *in* C. Castets-Renard (dir.), *Quelle protection des données personnelles en Europe ?*, Bruxelles, Larcier, 2015, pp. 91-92.

démontrer que ces données sont bien souvent utilisées comme « contrepartie » en l'échange de l'utilisation d'un service « gratuit » (pensons notamment aux réseaux sociaux, aux plateformes de vidéos ou aux moteurs de recherche), il n'en reste pas moins que le droit à la protection des données est un droit fondamental[26] qui ne peut, *a priori*, être cédé. Admettre le contraire reviendrait à reconnaître une forme de droit de propriété sur les données à caractère personnel et impliquerait que celles-ci soient cessibles. Or, selon le contrôleur européen de la protection des données, dès lors que ces données constituent une partie intégrante de notre être, celles-ci doivent par conséquent demeurer incessibles[27], au même titre que d'autres parties de notre corps, telles que nos organes[28].

Ce débat entre réalité du terrain et principes juridiques demeure cependant vif, dès lors que la Commission européenne a indiqué dans sa communication intitulée « Une nouvelle donne pour les consommateurs » qu'il existe « des lacunes dans la protection des consommateurs dans le cas des *services numériques "gratuits" pour lesquels ils doivent fournir des données à caractère personnel au lieu de payer une somme d'argent* »[29] (nous soulignons). De fait, une telle affirmation semble impliquer que la Commission estime qu'il soit possible de « payer » avec des données à caractère personnel[30].

10. Enfin, il convient de mentionner que la Commission a adopté une proposition de règlement dit « ePrivacy »[31], destiné à assurer le respect du droit à la vie privée, au secret des communications et à la protection des données à caractère personnel dans le cadre de la fourniture et de l'utilisation de services de communications électroniques[32]. Il conviendra donc également d'être attentif à l'articulation de cette réglementation, que nous n'analyserons pas ici, avec le RGPD.

B. Propriété intellectuelle

11. En droit européen, la protection de la propriété intellectuelle est conférée par plusieurs instruments juridiques. D'une part, le droit d'auteur[33] est

26 Ce droit est consacré par l'article 8 de la Convention européenne des droits de l'homme et l'article 8 de la Charte des droits fondamentaux de l'Union européenne.

27 CEPD, Avis 8/2018 sur le paquet législatif « Une nouvelle donne pour les consommateurs », 5 octobre 2018, pp. 14-15.

28 CEPD, Avis 4/2017 sur la proposition de directive concernant certains aspects des contrats de fourniture de contenu numérique, 14 mars 2017, p. 7.

29 Communication de la Commission au Parlement européen, au Conseil et au Comité économique et social européen, intitulée « Une nouvelle donne pour les consommateurs », Bruxelles, 11 avril 2018, COM(2018) 183 final, p. 6.

30 CEPD, Avis 8/2018, *op. cit.*, p. 14.

31 Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »), 10 janvier 2017, Bruxelles, COM(2017) 10 final.

32 Article 1er, § 1er, de la proposition de règlement « vie privée et communications électroniques ».

33 Pour une contribution relative à l'impact du numérique sur le droit d'auteur, voy., dans cet ouvrage, Fl. Jacques, M. Lognoul et B. Michaux, « Le droit d'auteur dans le marché numérique », pp. 7-52.

protégé par la directive 2001/29 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information[34]. D'autre part, il existe principalement deux directives spécifiques : la directive 96/9 sur la protection juridique des bases de données[35] et la directive 2009/24/CE concernant la protection juridique des programmes d'ordinateur[36].

La Belgique a transposé ces différents instruments juridiques dans son Code de droit économique[37].

1. *Droit d'auteur*

12. Les données, en tant que telles, ne sont pas protégées par le droit d'auteur[38]. Seule l'expression concrète d'un contenu sémantique extrait de données pourrait être protégée, si les conditions d'octroi de la protection par le droit d'auteur sont remplies[39]. À cet égard, l'information doit être mise en forme et originale pour être candidate à la protection par le droit d'auteur. La première condition nécessite une possibilité concrète d'appréhension de l'information. Si la condition de matérialisation ne pose *a priori* pas d'obstacle pour les données, il en est autrement de la condition d'originalité.

Définie par la Cour de justice de l'Union européenne comme étant une « création intellectuelle propre à son auteur »[40], l'originalité requiert que l'information soit le résultat de choix libres et créatifs reflétant la personnalité de l'auteur[41]. À titre d'illustration, si les actualités sont des données factuelles relatives à des évènements de notre société, il importe qu'elles soient communiquées de manière originale par le journaliste. L'information brute en tant que telle n'est alors pas protégée, mais l'expression choisie par le journaliste pourra bénéficier du droit d'auteur[42]. L'article 2, § 8, de la Convention de Berne confirme cette distinction en disposant que : « La protection de la présente Convention ne s'applique pas aux nouvelles du jour ou aux faits divers qui ont le caractère de simples informations de presse. » Si les deux conditions sont remplies, la donnée est alors susceptible de protection par la

34 Directive 2001/29/CE du Parlement européen et du Conseil sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, 22 mai 2011, *J.O.*, L 167.

35 Directive 96/9/CE du Parlement européen et du Conseil concernant la protection juridique des bases de données, 11 mars 1996, *J.O.*, L 77.

36 Directive 2009/24/CE concernant la protection juridique des programmes d'ordinateur, 23 avril 2009, *J.O.*, L 111.

37 Voy. principalement les articles XI.165 et s. Les dispositions spécifiques relatives au droit des bases de données se trouvent aux articles XI.186 et s. ainsi qu'aux articles XI.305 et s. En ce qui concerne la protection des programmes d'ordinateur, voy. les articles XI.294 et s.

38 N. Duch-Brown, B. Martens et F. Mueller-Langer, « The economics of ownership, access and trade in digital data », *Digital Economy Working Paper*, 2016-10, JRC Technical Reports, p. 7, disponible sur https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2914144.

39 *Ibid.*

40 C.J.C.E., 16 juillet 2009, *Infopaq International A/S c. Danske Dagblades Forening*, affaire C-5/08, EU:C:2009:465.

41 À ce sujet, voy. B. Michaux, « L'originalité en droit d'auteur, une notion davantage communautaire après l'arrêt *Infopaq* », *A.M.*, 2009/5, pp. 473-488.

42 M. Buydens, « Droit d'auteur et internet », disponible sur www.belspo.be/belspo/organisation/publ/pub_ostc/d_auteur/rapp_fr.pdf, 1999, p. 16.

loi relative au droit d'auteur, sans considération de sa nature technique ou scientifique[43].

13. Le droit d'auteur relatif aux bases de données permet, quant à lui, de protéger une sélection et un agencement original des données. En effet, l'article 3 de la directive 96/9 concernant la protection juridique des bases de données dispose que : « les bases de données qui, par le choix ou la disposition des matières, constituent une création intellectuelle propre à leur auteur sont protégées comme telle par le droit d'auteur. Aucun autre critère ne s'applique pour déterminer si elles peuvent bénéficier de cette protection. » Soulignons que l'article se poursuit en indiquant que : « La protection des bases de données par le droit d'auteur prévue par la présente directive ne couvre pas leur contenu et elle est sans préjudice des droits subsistant sur ledit contenu. » La protection ne s'applique dès lors pas directement aux données, mais permet un contrôle de leur accès.

La Cour de justice a été appelée à appliquer l'article 3 de la directive à un calendrier de rencontres footballistiques[44]. La Cour précise que seul le critère d'originalité doit être retenu dans la sélection et l'agencement des données[45]. Il convient dès lors de vérifier que des choix libres et créatifs ont été opérés par le concepteur de la base de données en se détachant de contraintes purement techniques et organisationnelles[46]. Dans la même veine, les efforts intellectuels fournis, le savoir-faire et le travail du créateur demeurent absents de l'appréciation[47].

2. *Droit « sui generis » sur les bases de données*

14. Les données seront rarement appréhendées en tant que bien isolé, et feront souvent partie d'une base de données. Au sein de l'Union européenne, les bases de données sont définies comme un « recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique et individuellement accessibles par des moyens électroniques ou d'une autre manière »[48].

Outre une protection par le droit d'auteur, la directive 96/9/CE octroie un droit *sui generis* sur le contenu de la base de données[49]. Ce droit protège uniquement la base de données prise dans son ensemble, et non les données prises individuellement[50]. La visée plus économique de celui-ci a justifié le

43 *Ibid.*, p. 15.
44 C.J.U.E., 1er mars 2012, *Football Dataco Ltd e.a. c. Yahoo! UK Ltd e.a.*, affaire C-604/10, EU:C:2012:115.
45 *Ibid.*, pt 40.
46 *Ibid.*, pts 38-39.
47 *Ibid.*, pt 46.
48 Article 1er, § 2, de la directive 96/9.
49 Articles 7 à 11 de la directive 96/9. Pour le droit belge, voy. les articles XI. 305 et s. du Code de droit économique.
50 N. Duch-Brown, B. Martens et F. Mueller-Langer, « The Economics of Ownership, Access and Trade in Digital Data », *op. cit.*, p. 14.

remplacement de la condition d'originalité par une condition d'existence d'un investissement financier, humain ou technique substantiel par le fabricant de la base de données.

La directive a vocation à bénéficier au fabricant de la base de données qui parvient à démontrer que « l'obtention[51], la vérification[52] ou la présentation[53] de ce contenu attestent un investissement substantiel du point de vue qualitatif ou quantitatif »[54]. À l'inverse, un investissement substantiel dans la création d'une base de données n'engendrera pas de protection par le biais du droit *sui generis*[55]. La législation européenne entend ainsi stimuler la mise en place de systèmes de stockage et de traitement d'informations existantes, et non pas la création elle-même[56].

À cet égard, la Cour de justice a antérieurement exclu de la protection par le droit *sui generis* un calendrier de courses hippiques en arguant que les investissements substantiels concernaient la création de données et non leur obtention[57]. En effet, la Cour n'a pas tenu compte des investissements consacrés à la composition des listes des chevaux participants, notamment l'occupation d'une trentaine de personnes chargées des inscriptions et de l'attribution d'un numéro de casaque et une stalle de départ[58]. Au motif de se situer dans la phase de création des données, le même sort a été attribué aux investissements réservés aux vérifications préalables à l'inscription portant sur l'identité de la personne y procédant, sur les caractéristiques et qualifications du cheval, de son propriétaire et du jockey[59]. La Cour appelle à la démonstration d'un investissement substantiel autonome par rapport aux moyens mis en œuvre pour la création des données[60].

Dans un arrêt ultérieur, la Cour a également qualifié de moyens portant sur la création des données les investissements attribués à l'élaboration d'un calendrier de rencontres footballistiques[61].

Par ailleurs, le législateur européen, dans son considérant 46, précise que « l'existence d'un droit d'empêcher l'extraction et/ou la réutilisation non autorisées de la totalité ou d'une partie substantielle d'œuvres, de données ou d'éléments d'une base de données ne donne pas lieu à la création d'un nouveau droit sur ces œuvres, données ou éléments mêmes ».

51 Par obtention, on entend la recherche d'éléments existants.
52 Par vérification, on entend la vérification de l'exactitude des informations contenues dans la base de données ainsi que son fonctionnement permanent.
53 Par présentation, on entend la disposition et l'organisation des éléments composant la base de données.
54 Article 7, § 1er, de la directive 96/9.
55 C.J.C.E., 9 novembre 2004, *The British Horseracing Board Ltd e.a c. William Hill Organization Ltd*, affaire C-203/02, EU:C:2004:695.
56 Considérant 12 de la directive 96/9.
57 C.J.C.E., 9 novembre 2004, *The British Horseracing Board*.
58 *Ibid.*, pts 37-38.
59 *Ibid.*, pts 39-40.
60 *Ibid.*, pt 35.
61 C.J.U.E., 1er mars 2012, *Football Dataco*, pt 36.

15. Le droit *sui generis* permet au titulaire du droit de contrôler les extractions et réutilisations de parties substantielles de sa base de données, appréciées quantitativement ou qualitativement[62]. Ainsi, le fabricant peut s'opposer à tout transfert permanent ou temporaire du contenu de sa base de données sur un autre support par quelque moyen ou sous quelque forme que ce soit et à toute forme de mise à disposition du public de la base de données[63].

Par ailleurs, la loi empêche les extractions et réutilisations de parties non substantielles, mais effectuées de manière répétée et systématique[64].

Le caractère substantiel des actes illicites s'apprécie tant au regard de la quantité volumétrique de données extraites ou réutilisées qu'en fonction de la valeur économique de la donnée. Par valeur économique sont visées les données ayant nécessité un investissement humain, financier ou technique particulièrement important pour le fabricant. *A contrario*, la valeur intrinsèque de la donnée en tant que telle n'est pas suffisante[65].

16. Bien que le droit *sui generis* ait pour finalité de protéger à la fois un contenu apprécié dans son ensemble, il convient de souligner que celui-ci semble néanmoins également et de permettre une certaine réservation de données particulières. Les évolutions jurisprudentielles récentes de la Cour de justice semblent mettre en lumière cette dualité. Dans l'affaire *Freistaat Bayern*[66], la Cour de justice a été amenée à affiner les contours de la notion même de « données ». Le litige au principal portait sur une accusation de reprise de données de cartes topographiques élaborées et publiées par le Land de Bavière à l'encontre de l'éditeur autrichien, Verlag Esterbauer.

L'affaire appelle une double question. Premièrement, il s'agit de déterminer si une extraction de données, au sens de la loi, était effectivement en cause. Dans l'affirmative, ladite extraction relèverait alors du champ d'application de la directive. Deuxièmement, il s'agit de se prononcer sur l'éventuel caractère illicite de l'extraction.

Pour répondre à la première question, la Cour rappelle sa jurisprudence *Fixture Marketing*[67]. Pour rencontrer la notion d'« éléments indépendants », elle insiste sur leur caractère « séparable les uns des autres » sans que la valeur informative de leur contenu s'en trouve affectée[68]. L'indépendance se voit être intimement liée à la préservation d'une valeur informative autonome. En effet, la Cour relève qu'une donnée peut voir sa valeur augmentée par son croisement avec d'autres informations se trouvant également dans la

62 Article 7 de la directive 96/9. Pour le droit belge, voy. l'article XI. 306 du Code de droit économique.
63 Article 7, § 2, de la directive 96/9.
64 Article 7, § 5, de la directive 96/9.
65 C.J.C.E., 9 novembre 2004, *The British Horseracing Board*, pts 70-72.
66 C.J.U.E., 29 octobre 2015, *Freistaat Bayern c. Verlag Esterbauer GmbH*, affaire C-490/14, EU:C:2015:735.
67 C.J.C.E., 9 novembre 2004, *Fixtures Marketing Ltd c. Organismos prognostikon agonon podosfairou AE (OPAP)*, affaire C-444/02, EU:C:2004:697.
68 C.J.U.E., 29 octobre 2015, *Freistaat Bayern*, pts 21-23.

base de données[69]. Consciente que ladite valeur peut être diminuée par une extraction et une isolation de la base source, la Cour n'y voit cependant pas un obstacle absolu et s'intéresse à la conservation d'une valeur informative autonome[70]. Pour apprécier cette dernière, la Cour décide de ne pas se faire juge des intentions du fabricant de la base de données et du réutilisateur. En conséquence, la qualité de cette valeur dépend de son intérêt pour le tiers à l'exploitation[71].

En ce qui concerne la seconde question relative au caractère illicite de l'extraction, il revient au fabricant de la base de données de démontrer les investissements humains, techniques ou financiers ayant été nécessaires pour obtenir, vérifier ou présenter la donnée extraite.

17. Les considérations émises par la Cour de justice dans son arrêt *Esterbauer* quant à l'extraction qualitative ont eu pour conséquence indirecte de conférer au fabricant un certain droit sur une donnée individuelle. D'aucuns dénoncent, par les interventions successives de la Cour de justice, le glissement du droit *sui generis* des bases de données vers un droit sur la donnée en elle-même. En effet, l'arrêt *Fixture Marketing*[72] a consacré une valeur autonome à des données individuelles et non plus à un contenu apprécié dans son ensemble. Ensuite, par l'arrêt *BHB*[73], la Cour de justice met en exergue une extraction illicite d'une petite quantité de données au regard des investissements encourus. Cette approche est ensuite renforcée par l'arrêt *Esterbauer*[74].

18. Par ailleurs, les limites du champ d'application du droit *sui generis* emportent également une possible réservation contractuelle de la donnée. À titre d'exemple, relevons l'arrêt *Ryanair*[75]. L'affaire portée devant la Cour de justice concernait un site internet de comparateur de prix de compagnies *low cost* avec la possibilité additionnelle d'effectuer une réservation. Le site fonctionne par l'agrégation d'informations provenant des sites internet des compagnies aériennes proposées à la réservation. Cependant, les conditions générales de Ryanair interdisent à autrui de donner la faculté aux internautes d'effectuer des réservations sur un autre site internet. En outre, Ryanair oblige la conclusion d'une licence pour l'utilisation de systèmes automatisés ou de logiciels permettant l'extraction de données.

La Cour d'appel d'Amsterdam semble reconnaître implicitement un droit d'auteur au bénéfice de la société irlandaise en jugeant que le site de comparateur de prix bénéficie de l'exception légale d'usage normal de la base

69 *Ibid.*, pt 23.
70 *Ibid.*, pt 24.
71 *Ibid.*, pt 27.
72 C.J.C.E., 9 novembre 2004, *Fixtures Marketing*.
73 C.J.C.E., 9 novembre 2004, *The British Horseracing Board*.
74 Sur ce point, voy. B. MICHAUX, « La Cour de justice favorise-t-elle l'appropriation des données par celui qui les a traitées ? », note sous C.J.U.E. (2e ch.), 29 octobre 2015, *A&M*, 2017, pp. 28-34.
75 C.J.U.E., 15 janvier 2015, *Ryanair Ltd c. PR Aviation BV*, affaire C-30/14, EU:C:2015:10.

de données. En revanche, Ryanair ne peut invoquer un droit *sui generis* en l'absence de preuves suffisantes d'investissements substantiels pour l'obtention, la vérification et la présentation des données.

En de telles circonstances, la juridiction hollandaise posa, à la Cour de justice, une question préjudicielle portant sur l'applicabilité des exceptions mises en place par la directive 96/9 au bénéfice des utilisateurs légitimes et de la marge de manœuvre contractuelle laissée au détenteur de la base de données.

En substance, la Cour de justice précise que les articles créant des exceptions et leur conférant un caractère impératif sont étroitement liés au régime de protection auquel ils se rattachent, à savoir respectivement la protection par le droit d'auteur et par le droit *sui generis*[76]. Par conséquent, en l'absence de protection effective, la directive 96/9 ne fait pas obstacle à l'adoption de clauses contractuelles conditionnant l'utilisation de la base de données concernée et, partant, limite les possibilités pour un utilisateur subséquent[77]. La base de données – et les données y contenues – a alors une nature hybride. Son caractère libre de droits est amoindri par une possible largesse dans la limitation contractuelle.

3. *Text and data mining*

a) Utilité de l'adoption d'une nouvelle exception

19. Une nouvelle exception obligatoire pour tous les États membres de l'Union européenne a été récemment adoptée par le trilogue, à savoir le *text and data mining* (ci-après « TDM »). L'article 2, § 2, de la proposition de directive[78] définit le TDM comme « toute technique d'analyse automatisée visant à analyser du texte et des données sous forme numérique afin de générer de l'information, y compris, mais sans s'y limiter, des modèles, tendances et corrélations »[79]. Le TDM est un mécanisme permettant aux logiciels de lire et d'analyser de grandes quantités de contenus numériques (textes, images, etc.) afin d'en extraire des informations. L'utilité de cet outil est de permettre l'examen de grandes quantités de données en un temps record,

76 *Ibid.*, pt 39.

77 *Ibid.*, pts 39-40.

78 Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market, 20 février 2019, n° 6637/19 (ci-après : proposition n° 6637/19). Voy. les textes suivants adoptés par le Parlement européen le 26 mars 2019 : (i) Résolution législative du Parlement européen du 26 mars 2019 sur la proposition de directive du Parlement européen et du Conseil sur le droit d'auteur dans le marché unique numérique (COM(2016)0593 – C8-0383/2016 – 2016/0280(COD)) (Procédure législative ordinaire: première lecture) ; (ii) Position du Parlement européen arrêtée en première lecture le 26 mars 2019 en vue de l'adoption de la directive (UE) 2019/... du Parlement européen et du Conseil sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE. Ces textes sont consultables à l'adresse suivante (dernièrement consultée le 6 avril 2019) : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2019-0231+0+DOC+XML+V0//FR#top.

79 La définition officielle en anglais est formulée de la manière suivante : « any automated analytical technique aiming to analyse text and data in digital form in order to generate information, including, but not limited to, patterns, trends and correlations ».

dépassant ainsi les capacités humaines[80]. Si cette exception est relative au droit d'auteur, il nous paraît qu'elle aura un impact certain pour les fabricants des bases de données.

20. La mise en place d'une telle exception ne semble pas anodine. En effet, ériger le TDM en exception aux prérogatives du titulaire des droits d'auteur laisse supposer qu'une telle pratique serait par nature une atteinte au cadre légal. Or, on pourrait arguer, en faveur du TDM, qu'il s'intéresse à l'information qui, rappelons-le, est en principe libre de droit, et non pas à son enveloppe corporelle, celle-ci étant en revanche protégeable.

En réalité, la vigilance s'impose, car il n'est pas toujours aisé de distinguer l'information de son support. La pratique du TDM entraîne alors des actes de reproduction d'œuvres protégées ou de parties de celles-ci par la réalisation de copies nécessaires à l'analyse.

Une autre hypothèse de manipulation contraire au droit d'auteur serait le changement de format de la donnée opérée afin de permettre sa lisibilité par le logiciel dédié au TDM[81].

Par conséquent, il est nécessaire d'examiner l'espace de liberté que les exceptions actuellement en vigueur accordent aux pratiques de l'exploration de textes et de données.

21. Une première possibilité serait l'exception prévue pour permettre les actes de reproduction temporaires[82]. La directive 2001/29/CE autorise les actes de reproduction temporaire qui sont transitoires ou accessoires, qui font partie intégrante et essentielle d'un procédé technique et dont le seul but est de permettre la transmission sur un réseau entre tiers par un intermédiaire ou une utilisation licite d'une œuvre protégée, et qui n'ont aucune signification économique propre[83]. Si rien n'empêche l'applicabilité de cette exception au TDM, la vigilance demeure. En effet, dans certaines circonstances, l'applicabilité de cette exception semble incertaine. Selon la technique utilisée, les copies peuvent être permanentes et il n'est pas certain qu'elles soient dépourvues de toute signification économique indépendante. En effet, les copies réalisées sont inhérentes à la découverte d'une nouvelle connaissance qui pourrait être exploitée économiquement[84].

80 Ch. Geiger, G. Frosio et O. Bulayenko, « Crafting a Text and Data Mining Exception for Machine Learning and Big Data in the Digital Single Market », *in* X. Seuba, Ch. Geiger et J. Pénin (dir.), *Intellectual Property and Digital Trade in the Age of Artificial Intelligence and Big Data*, Suisse, International Centre for Trade and Sustainable Development (ICTSD), 2018, p. 97.

81 I.A. Stamatoudi, « Text and Data Mining », *in* I.A. Stamatoudi (dir.), *New Developments in EU and International Copyright Law*, Bruxelles, Kluwer, 2016, p. 263.

82 Considérant 8 de la proposition n° 6637/19.

83 Article 5, § 1er, de la directive 2001/29/CE du Parlement européen et du Conseil sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, 22 mai 2001, *J.O.*, L 167.

84 C. Bernault, « Le cas particulier du text and data mining », *in* C. Bernault (dir.), *Open access et droit d'auteur*, Bruxelles, Larcier, 2016, pp. 180-186. Voy. également, I.A. Stamatoudi, « Text and Data Mining », *op. cit.* ;

En revanche, l'exception de reproduction provisoire pourrait s'appliquer à un mécanisme de TDM ne faisant pas acte de copie, mais uniquement d'exploration. Dans une telle hypothèse, les actes de reproduction ne seraient que provisoires et partie intégrante du procédé d'exploration[85]. Toutefois, nous le verrons, le droit *sui generis* vient nuancer le propos.

22. Si la copie faite lors de l'exploration est une copie complète de l'œuvre en question, l'exception de citation ne peut être invoquée. Par ailleurs, l'exception de l'illustration pour la recherche scientifique paraît également inadéquate puisque la recherche est la raison de la reproduction[86].

23. De surcroît, le TDM pourrait résulter en des actes d'extraction et de réutilisation tant quantitatifs que qualitatifs des données contenues dans différentes bases de données[87]. En effet, l'exploration de la base de données ainsi que l'utilisation de son contenu pourraient répondre à la définition de la notion d'extraction en ce qu'il s'agit d'un transfert permanent ou temporaire sur un autre support. À cet égard, il n'est pas inutile de rappeler la jurisprudence *Innoweb* par laquelle la Cour de justice condamne un métamoteur de recherche explorant l'intégralité de diverses bases de données afin de communiquer aux internautes les résultats correspondants les plus adéquats au regard de leur recherche. La Cour y décèle une mise à disposition illégale, à défaut d'autorisation préalable, du contenu des bases de données utilisées[88].

24. Il convient désormais d'analyser l'adéquation et l'efficacité des exceptions prévues par la directive aux utilisateurs légitime. En premier lieu, l'article 9, b, de la directive 96/9 dispose que « les États membres peuvent établir que l'utilisateur légitime d'une base de données qui est mise à la disposition du public de quelque manière que ce soit peut, sans autorisation du fabricant de la base, extraire et/ou réutiliser une partie substantielle du contenu de celle-ci : [...] lorsqu'il s'agit d'une extraction à des fins d'illustration de l'enseignement ou de recherche scientifique, pour autant qu'il indique la source et dans la mesure justifiée par le but non commercial à atteindre ».

Plusieurs critiques peuvent être émises concernant l'applicabilité de cette exception. Premièrement, les disparités nationales relatives aux différentes conditions d'application empêchent une approche harmonisée au sein de l'Union européenne. Deuxièmement, il n'est pas certain qu'il soit techni-

Ch. Geiger, G. Frosio et O. Bulayenko, « Crafting a Text and Data Mining Exception for Machine Learning and Big Data in the Digital Single Market », *op. cit.*

85 I.A. Stamatoudi, « Text and Data Mining », *op. cit.*, pp. 268-271.

86 Sur la pratique des contrats d'édition, voy. C. Bernault, « Le cas particulier du text and data mining », *op. cit.*, pp. 177 et s.

87 C. Bernault, « Le cas particulier du text and data mining », *op. cit.*, p. 173. Voy. également I.A. Stamatoudi, « Text and Data Mining », *op. cit.*, pp. 265-266 ; Ch. Geiger, G. Frosio et O. Bulayenko, « Crafting a Text and Data Mining Exception for Machine Learning and Big Data in the Digital Single Market », *op. cit.*, pp. 98-99.

88 C.J.U.E., 19 décembre 2013, *Innoweb BV c. Wegener ICT Media BV et Wegener Mediaventions BV*, affaire C-202/12, EU:C:2013:850, pt 50.

quement et humainement possible d'indiquer la source de chaque information extraite d'une base de données. Troisièmement, l'exigence d'un but non commercial pourrait poser des difficultés d'interprétation en fonction de l'organisation et des mécanismes de financements des différents centres de recherches existants au sein de l'Union européenne[89].

25. En second lieu, le législateur européen met en place l'exception d'usage normal. L'article 6, § 1er, de la directive 96/9 dispose que :

> « L'utilisateur légitime d'une base de données ou de copies de celle-ci peut effectuer tous les actes visés à l'article 5 qui sont nécessaires à l'accès au contenu de la base de données et à son utilisation normale par lui-même sans l'autorisation de l'auteur de la base. Dans la mesure où l'utilisateur légitime est autorisé à utiliser une partie seulement de la base de données, le présent paragraphe s'applique seulement à cette partie. »

En l'absence de jurisprudence, l'interprétation à conférer à la condition de normalité, il n'est pas certain que le TDM puisse répondre à l'exception[90].

26. En troisième lieu, en marge du droit d'auteur et du droit *sui generis*, la possibilité d'interdire contractuellement le TDM lorsque la base de données ne remplit pas les conditions de protection est un frein non négligeable[91].

b) Modification législative

27. Soucieuse du vide juridique entourant cette situation, l'idée est apparue à la Commission européenne d'introduire, lors de sa révision de la directive 2001/29/CE, une exception obligatoire pour tous les États membres en faveur du TDM. En substance, elle permet aux organismes de recherche d'intérêt public d'appliquer des techniques d'exploration de textes et de données à des contenus qui leur sont légalement accessibles à des fins de recherche scientifique[92].

La disposition est libellée comme suit :

> « Member States shall provide for an exception to the rights provided for in Article 2 of Directive 2001/29/EC, Articles 5(a) and 7(1) of Directive 96/9/EC and Article 11(1) of this Directive for reproductions and extractions made by research organisations and cultural heritage institutions in order to carry out text and data mining of works or other subject-matter to which they have lawful access, for the purposes of scientific research.
>
> Copies of works or other subject-matter made in compliance with paragraph 1 shall be stored with an appropriate level of security and may be retained for the purposes of scientific research, including for the verification of research results.

89 I.A. Stamatoudi, « Text and Data Mining », *op. cit.*, pp. 271-277.

90 *Ibid.*, pp. 277-278 ; Ch. Geiger, G. Frosio et O. Bulayenko, « Crafting a Text and Data Mining Exception for Machine Learning and Big Data in the Digital Single Market », *op. cit.*, p. 102.

91 I.A. Stamatoudi, « Text and Data Mining », *op. cit.*, p. 267.

92 Article 3 de la proposition n° 6637/19.

> Rightholders shall be allowed to apply measures to ensure the security and integrity of the networks and databases where the works or other subject-matter are hosted. Such measures shall not go beyond what is necessary to achieve that objective.
>
> Member States shall encourage rightholders and, research organisations and cultural heritage institutions to define commonly-agreed best practices concerning the application of the obligation and measures referred to respectively in paragraphs 1a and 3 ».

Cette modification du cadre juridique européen aurait pour effet de contraindre le titulaire de droit à l'ouverture de ses données. Celle-ci est toutefois limitée par un champ d'application restreint à la recherche scientifique. L'article 2, 1°, de la proposition n° 6637/19 définit l'organisme de recherche en indiquant qu'il peut s'agir « d'une université, d'un institut de recherche ou tout autre organisme ayant pour objectif premier de mener des recherches scientifiques, ou de mener des recherches scientifiques et de fournir des services éducatifs : (a) à titre non lucratif ou en réinvestissant tous les bénéfices dans ses recherches scientifiques ou (b) dans le cadre d'une mission d'intérêt public reconnue par un État membre[93] ; de telle manière qu'il ne soit pas possible pour une entreprise exerçant une influence déterminante sur cet organisme de bénéficier d'un accès privilégié aux résultats produits par ces recherches scientifiques »[94]. En outre, la proposition de directive précise que les universités et instituts de recherches peuvent avoir recours aux techniques de TDM dans le cadre de partenariats public-privé[95].

28. En parallèle, une seconde exception est prévue[96]. Cette dernière n'est pas obligatoire et son implémentation dans l'ordre juridique national est laissée à l'appréciation de chaque État membre. Cette exception n'est plus limitée à la recherche scientifique et permet, plus largement, au secteur privé d'avoir recours aux TDM pour des œuvres légalement accessibles et pour lesquels les titulaires de droit d'auteur ou de droit *sui generis* n'ont pas interdit le TDM.

C. Secrets d'affaires

29. Un autre pan du droit de l'Union européenne à prendre en considération, dès lors qu'il confère une forme de droit sur certaines données, est celui de la protection des secrets d'affaires[97], qui a été harmonisé en 2016 par

93 Considérant 11 de la proposition n° 6637/19.
94 Article 2, 1°, de la proposition n° 6637/19.
95 Considérant 11 de la proposition n° 6637/19.
96 À ce propos, voy. le considérant 13, a, de la proposition n° 6637/19.
97 Pour de plus amples développements quant à ce régime de protection, voy., dans cet ouvrage, V. Cassiers, « La protection des secrets d'affaires dans l'environnement numérique ».

le biais de l'adoption de la directive sur les secrets d'affaires[98], transposée en droit belge par une loi du 30 juillet 2018[99].

Contrairement au régime de protection des bases de données étudié ci-dessus, la protection des secrets d'affaires peut potentiellement s'appliquer à des données prises individuellement[100].

Toutefois, le champ de la protection octroyé est, une nouvelle fois, plutôt réduit[101]. De fait, la protection est limitée aux données pouvant être qualifiées de secrets d'affaires, à savoir :

> « [Une] information qui répond à toutes les conditions suivantes :
>
> a) Elle est secrète en ce sens que dans sa globalité ou dans la configuration et l'assemblage exacts de ses éléments, elle n'est pas généralement connue des personnes appartenant aux milieux qui s'occupent normalement du genre d'information en question, ou ne leur est pas aisément accessible ;
> b) Elle a une valeur commerciale parce qu'elle est secrète ;
> c) Elle a fait l'objet, de la part de la personne qui en a le contrôle de façon licite, de dispositions raisonnables, compte tenu des circonstances, destinées à la garder secrète »[102].

Par ailleurs, le détenteur des secrets d'affaires[103] se voit uniquement accorder une protection contre l'obtention, l'utilisation et la divulgation illicites[104], ce qui différencie ce régime de la protection relative au droit d'auteur et aux bases de données[105].

Au vu de la façon dont ce régime de protection est construit, deux éléments méritent d'être quelque peu étayés, à savoir la notion de « dispositions raisonnables destinées à garder l'information secrète », d'une part, et le caractère « illicite » de l'obtention, l'utilisation et/ou la divulgation du secret, d'autre part.

30. Le bénéfice de la protection de la réglementation relative aux secrets d'affaires est donc assujetti à la mise en place de « dispositions raisonnables, compte tenu des circonstances, destinées à garder [l'information] secrète »[106]. Malheureusement, ni la directive ni la loi belge de transposition ne fournissent plus de précisions quant aux mesures de protection devant être considérées

98 Directive 2016/943/UE du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites, *J.O.*, L 157/1, 15 juin 2016.
99 Loi du 30 juillet 2018 relative à la protection des secrets d'affaires, *M.B.*, 14 août 2018.
100 J. Drexl, « Designing Competitive Markets for Industrial Data », *op. cit.*, p. 23.
101 *Ibid.*
102 Article I.17/1, 1°, du Code de droit économique.
103 « Toute personne physique ou morale qui a le contrôle d'un secret d'affaires de façon licite » (article I.17/1, 2°, du Code de droit économique).
104 Article XI.332/1 du Code de droit économique.
105 I. Graef, *EU Competition Law, Data Protection and Online Platforms : Data as Essential Facility*, Alphen aan den Rijn, Kluwer, 2016, p. 141.
106 Article I.17/1, 1°, c), du Code de droit économique.

comme raisonnables. De même, le texte belge est trop récent pour avoir généré de la jurisprudence sur la question.

Néanmoins, il est utile de se référer à deux décisions adoptées dans d'autres États membres de l'Union, afin d'envisager le type de mesures techniques potentiellement recouvertes par le vocable de « dispositions raisonnables ». Ainsi, un tribunal espagnol[107] a considéré que les mesures adoptées afin de rendre l'information secrète doivent être « adéquates et raisonnables », et doivent être tant externes qu'internes[108]. Ce tribunal précise que les mesures externes doivent viser à empêcher aux tiers d'accéder à ces informations, tandis que les mesures internes doivent viser à limiter l'accès aux informations aux seuls employés ou collaborateurs qui doivent (ou devraient) en avoir connaissance et les traiter[109]. Dans la même veine, la Cour suprême autrichienne[110] a considéré que la mise en place de logs d'accès, requérant un nom d'utilisateur et un mot de passe, afin de limiter le nombre de personnes pouvant accéder à l'information, et afin d'identifier ces derniers, constituait une disposition raisonnable destinée à garder l'information secrète[111].

31. La législation belge est, en revanche, plus loquace sur le caractère « illicite » de l'obtention, l'utilisation et/ou la divulgation du secret. Ainsi, sera illicite l'obtention d'un secret, sans le consentement du détenteur, réalisée par le biais d'un accès non autorisé à tout document, objet, matériau, substance ou fichier électronique ou d'une appropriation ou copie non autorisée de ces éléments, ou par le biais de tout autre comportement qui, eu égard aux circonstances, est considéré comme contraire aux usages honnêtes en matière commerciale[112]. L'utilisation ou la divulgation d'un secret seront, quant à elles, considérées comme illicites lorsqu'elles sont réalisées, sans le consentement du détenteur, par une personne ayant obtenu le secret de façon illicite, ou ayant agi en violation d'un accord de confidentialité ou de toute autre obligation de ne pas divulguer le secret d'affaires, ou encore ayant agi en violation d'une obligation contractuelle ou de toute autre obligation limitant l'utilisation du secret d'affaires[113].

32. Enfin, notons que le droit belge précise également les cas dans lesquels l'utilisation de secrets d'affaires par un tiers est considérée comme licite[114], ce qui devrait permettre de renforcer la sécurité juridique relative à ces questions.

107 Tribunal provincial de Madrid (section 28), jugement civil n° 441/2016, *Rec.* 11/2015, 19 décembre 2016, inédit.

108 J. McClelland, S. Grimes et S. Murphy, « EU Trade Secrets Directive : What Are "Reasonable Steps" ? », 7 février 2019, disponible sur www.lexology.com/r.ashx?l=8BR0T2L.

109 *Ibid.*

110 Cour suprême autrichienne, décision n° 4 Ob 165/16t, 25 octobre 2016, disponible, en allemand, sur www.ogh.gv.at/entscheidungen/entscheidungen-ogh/eindringen-in-fremde-it-systeme-verstoesst-gegen-das-uwg/.

111 J. McClelland, S. Grimes et S. Murphy, « EU Trade Secrets Directive », *op. cit.*

112 Article XI.332/4, § 1er, du Code de droit économique.

113 Article XI.332/4, § 2, du Code de droit économique.

114 Articles XI.332/3 et XI.332/5 du Code de droit économique.

§ 2. Instruments juridiques limitant les droits sur les données, en favorisant leur circulation

33. Après avoir passé en revue les instruments juridiques principaux conférant des droits sur les données, il convient à présent d'étudier certains instruments qui, au contraire, limitent les droits sur celles-ci en vue de favoriser leur circulation. Cette volonté de favoriser le partage et la circulation de données est notamment portée par l'OCDE, selon laquelle les données devraient être considérées comme une ressource infrastructurelle, dès lors qu'elles sont des « moyens partagés à plusieurs fins »[115] qui, au vu de leur nature non rivale, peuvent servir pour de nombreux produits et services privés, publics et sociaux[116].

Pour des raisons d'économie, il ne nous est pas possible de passer en revue l'ensemble de ces instruments. Ce faisant, nous avons pris l'option de nous focaliser sur les deux instruments transversaux qui nous apparaissent comme étant les plus pertinents (A), ainsi que sur trois législations sectorielles que nous estimons être les plus abouties à ce stade (B).

A. Instruments transversaux

34. Deux instruments transversaux, à savoir des règles juridiques s'appliquant indépendamment du secteur d'activité, limitant les droits sur les données, en favorisant leur circulation, méritent d'être présentés dans cette contribution. Il s'agit du droit à la portabilité des données (1) et de l'interdiction des abus de position dominante (2).

1. Droit à la portabilité des données

35. Le concept de portabilité existe depuis longtemps déjà au niveau européen pour les numéros de téléphone[117], mais celui-ci a connu un regain d'intérêt suite à l'insertion, à l'article 20 du RGPD, d'un droit à la portabilité des données à caractère personnel[118].

115 *Shared means to many ends.*

116 OCDE, *Data-Driven Innovation : Big Data for Growth and Well-Being*, Paris, OECD Publishing, 2015, p. 179, disponible sur http://dx.doi.org/10.1787/9789264229358-en.

117 Article 30 de la directive 2002/22/CE du Parlement européen et du Conseil du 7 mars 2002 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, *J.O.*, 24 avril 2002, L 108/51 ; article 106 de la directive 2018/1972/UE du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (refonte), *J.O.*, 17 décembre 2018, L 321/36. Pour plus d'informations, voy. M. Ledger et Th. Tombal, « Le droit à la portabilité dans les textes européens : droits distincts ou mécanisme multi-facettes ? », *R.D.T.I.*, 2018/3, n° 72 (à paraître).

118 Pour une analyse détaillée de ce droit, voy. Th. Tombal, « Les droits de la personne concernée dans le RGPD », *op. cit.*, pp. 482-523 ; B. Van der Auwermeulen, « How to attribute the right to data portability in Europe : A comparative analysis of legislations », *Computer Law & Security Review*, 2017, n° 33, pp. 57-72 ; I. Graef, M. Hosovec et N. Purtova, « Data Portability and Data Control : Lessons for an Emerging Concept in EU Law », 15 décembre 2017, *Tilburg Law School Research Paper*, n° 2017/22, *TILEC Discussion Paper*, n° 2017-041, disponible sur http://ssrn.com/abstract=3071875.

L'objectif de ce droit est double. D'une part, il « représente [...] une opportunité de "rééquilibrer" la relation entre les personnes concernées et les responsables de traitements »[119], en rendant aux personnes concernées le contrôle sur les données à caractère personnel les concernant[120]. D'autre part, il permet à la personne concernée de pouvoir plus facilement changer de fournisseur de service[121]. La volonté est, en effet, d'éviter que les consommateurs ne soient « coincés »[122] par les géants actuels tels que Facebook ou Google, en leur permettant de « porter » certaines données vers un nouveau service alternatif en ligne.

36. Ce faisant, l'article 20 du RGPD confère à toute personne concernée le droit de recevoir les données à caractère personnel la concernant qu'elle a fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine[123]. Sont considérées comme « fournies » les « données activement et sciemment fournies par la personne concernée »[124] (nom, prénom, âge, adresse email...), ainsi que les « données observées fournies par la personne concernée grâce à l'utilisation du service ou du dispositif [du responsable de traitement] »[125] (historique de recherche, données de trafic et de localisation...). En revanche, ne seront pas soumises au droit à la portabilité « les données déduites et les données dérivées [qui] sont créées par le responsable de traitement sur la base des données "fournies par la personne concernée" »[126] (profils utilisateurs, résultats d'une évaluation de la santé de la personne concernée fondée sur les données de santé que sa montre intelligente a collectées...).

Si ce droit permet à la personne concernée de recevoir les données à caractère personnel la concernant, qu'elle a fournies à un responsable du traitement, en vue de les stocker pour son propre usage futur, il permet surtout à celle-ci de transmettre directement ces données d'un responsable de traitement à un autre, et ce, sans que le responsable de traitement originaire ne puisse y faire obstacle[127].

C'est en ce sens que ce droit à la portabilité des données limite les droits du responsable de traitement originaire sur les données, et en favorise la circulation, pour autant cependant que cela soit « techniquement possible »[128].

119 Groupe de travail « Article 29 », « Lignes directrices relatives au droit à la portabilité des données », WP 242 rev.01, 13 avril 2017, p. 4.
120 *Ibid.*
121 *Ibid.*
122 *Locked-in.*
123 Article 20, § 1er, du RGPD.
124 Groupe 29, « Lignes directrices relatives au droit à la portabilité des données », *op. cit.*, p. 12.
125 *Ibid.*
126 *Ibid.*
127 Article 20, § 2, du RGPD ; Groupe 29, « Lignes directrices relatives au droit à la portabilité des données », *op. cit.*, p. 5.
128 Article 20, § 2, du RGPD.

C'est notamment dans ce contexte que la recommandation contenue dans le considérant 68, mais non reprise dans l'article 20 du RGPD, invitant les responsables de traitement à fournir les données dans un format « interopérable »[129], prend tout son sens. Notons à cet égard que Google, Facebook, Microsoft et Twitter contribuent, aux côtés d'autres acteurs, au *Data Transfer Project*, né en 2017, dont le but est de créer une plateforme open source permettant la portabilité directe des données entre les fournisseurs de services participants[130].

37. Dans la lignée de la création de ce droit à la portabilité des données à caractère personnel, la Commission européenne a également envisagé d'instaurer un droit à la portabilité des données non personnelles, afin de favoriser la circulation de ces dernières[131].

Après réflexion, celle-ci n'a, pour l'heure, toutefois pas érigé de tel droit, et s'est limitée à encourager et à faciliter l'élaboration de codes de conduite, par autorégulation, pour le portage de données[132].

Ces codes doivent être fondés sur les principes de transparence et d'interopérabilité, et doivent tenir dûment compte des normes ouvertes[133]. Par ailleurs, ils devraient notamment contenir :

> « a) [Des] bonnes pratiques qui facilitent le changement de fournisseurs de services et le portage des données dans des formats structurés, usuels et lisibles par machine, notamment dans des formats standard ouverts, lorsque le fournisseur de services obtenant les données le demande ou l'exige ; [et]
>
> b) [Des] exigences minimales d'information afin que les utilisateurs professionnels disposent, préalablement à la conclusion d'un contrat de traitement des données, d'informations suffisamment détaillées, claires et transparentes en ce qui concerne les processus, les exigences techniques, les délais et les frais qui s'appliquent dans le cas où un utilisateur professionnel souhaite changer de fournisseur de services ou transférer ses données pour les rapatrier vers ses propres systèmes informatiques »[134].

129 L'interopérabilité est définie comme étant « la capacité de diverses organisations hétérogènes à interagir en vue d'atteindre des objectifs communs, mutuellement avantageux et convenus, impliquant le partage d'informations et de connaissances entre elles, selon les processus d'entreprise qu'elles prennent en charge, par l'échange de données entre leurs systèmes informatiques (TIC) respectifs » (article 2, 1°, de la proposition de décision du Parlement européen et du Conseil établissant un programme concernant des solutions d'interopérabilité pour les administrations publiques, les entreprises et les particuliers en Europe (ISA2) – L'interopérabilité comme moyen de moderniser le secteur public, 26 juin 2014, COM(2014) 367 final, disponible sur http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52014PC0367).
130 Voy. https://datatransferproject.dev/. Notons également que Google permet à toute personne titulaire d'un compte Google de télécharger les données que cet opérateur possède à son sujet. Pour ce faire, il suffit pour cette personne de se rendre dans la section « Informations personnelles et confidentialité » de son compte Google, d'ouvrir la sous-section « Définir votre contenu », et de cliquer sur « Télécharger vos données ».
131 Communication de la Commission, « Créer une économie européenne fondée sur les données », *op. cit.*, pp. 17-18.
132 Article 6, § 1er, du règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, *J.O.*, L 303/59, 28 novembre 2018.
133 *Ibid.*
134 *Ibid.*

Afin d'assurer une représentativité parmi les entreprises collaborant à l'élaboration de ces codes de conduite, qui seront vraisemblablement adoptés par secteur, la Commission devra veiller à ce que toutes les parties intéressées (PME, start-ups et fournisseurs de services clouds…) soient impliquées[135].

Enfin, la Commission devra encourager ces parties à finaliser la rédaction de ces codes de conduites pour le 29 novembre 2019 au plus tard, et les inciter à ce que ceux-ci soient mis en œuvre le 29 mai 2020 au plus tard[136].

2. *Interdiction des abus de position dominante*

38. À l'instar du droit à la portabilité des données, le droit de la concurrence pourrait potentiellement également être utilisé pour limiter les droits de certaines entreprises sur leurs données. Ainsi, la Commission européenne indiquait dans sa communication intitulée « Créer une économie européenne fondée sur les données » que :

> « Dans certains cas, les fabricants ou les prestataires de services peuvent devenir les propriétaires "de fait" des données que leurs machines ou leurs processus génèrent, même si ces machines sont la propriété de l'utilisateur. Le contrôle "de fait" de ces données peut représenter un facteur de différenciation et un avantage concurrentiel pour les fabricants »[137].

Il est, en effet, pertinent de se demander si un tel contrôle « de fait » des données – duquel pourraient découler un droit d'usage exclusif « de fait » des données et un droit sous-jacent de prévention de l'accès auxdites données par un tiers – pourrait mener à un abus de position dominante, interdit par l'article 102 du TFUE[138].

39. Plus particulièrement se pose la question de savoir si la jurisprudence de la Cour de justice de l'Union européenne relative à la « théorie des facilités essentielles »[139] pourrait être appliquée dans cette hypothèse, ce qui a fait l'objet de nombreuses contributions doctrinales[140].

135 Article 6, § 2, du règlement 2018/1807.

136 Article 6, § 3, du règlement 2018/1807.

137 Communication de la Commission, « Créer une économie européenne fondée sur les données », *op. cit.*, p. 12.

138 Traité sur le fonctionnement de l'Union européenne, *J.O.*, C 326/47, 26 octobre 2012.

139 Trib., 17 septembre 2007, *Microsoft Corp. c. Commission of the European Communities*, T-201/04, EU:T:2007:289 ; C.J.C.E., 29 avril 2004, *IMS Health GmbH & Co. OHG c. NDC Health GmbH & Co. KG*, affaire C-418/01, EU:C:2004:257 ; C.J.C.E., 26 novembre 1998, *Oscar Bronner GmbH & Co. KG c. Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG, Mediaprint Zeitungsvertriebsgesellschaft mbH & Co. KG and Mediaprint Anzeigengesellschaft mbH & Co. KG*, affaire C-7/97, EU:C:1998:569 ; C.J.C.E., 6 avril 1995, *Radio Telefis Eireann (RTE) and Independant Television Publications LTD (ITP) c. Commission of the European Communities*, affaires jointes C-241/91 et C-242/91, EU:C:1995:98.

140 Voy., *inter alia*, I. Graef, EU Competition Law, Data Protection and Online Platforms, *op. cit.* ; I. Graef, « Market Definition and Market Power in Data : The Case of Online Platforms », *World Competition Law and Economics Review*, 2015, vol. 38, n° 4, pp. 473-506 ; J. Drexl, « Designing Competitive Markets for Industrial Data », *op. cit.*, pp. 44-55 ; G. Colangelo et M. Maggiolino, « Big data as misleading facilities », *European Competition Journal*, 2017, n° 13, vol. 2-3, pp. 249-281 ; I. Graef, S. Wahyuningtyas et P. Valcke, « Assessing data access issues in online platforms », *Telecommunications Policy*, 2015, vol. 39, p. 382 ; Autorité de la concurrence et Bundeskartellamt, « Competition Law and Data », 10 mai 2016, disponible sur www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf ; H. Schweitzer, J. Haucap, W. Kerber et R. Welker, « Modernising the Law on Abuse of Market Power », Report for the Federal Ministry for Economic Affairs and Energy (Germany), 29 août 2018, disponible sur www.bmwi.de/Redaktion/DE/Downloads/Studien.

141 D. Geradin, A. Layne-Farrar et N. Petit, *EU Competition Law and Economics*, Oxford, Oxford University Press, 2012, p. 256 ; N. Petit, « L'arrêt *Microsoft*. Abus de position dominante, refus de licence et vente liée… L'article 82 sans code source », *J.D.E.*, 2008, p. 9.

142 Autorité de la concurrence et Bundeskartellamt, « Competition Law and Data », *op. cit.*, p. 18. Traduction libre.

143 Autorité belge de la concurrence, décision n° BMA-2015-P/K-27-AUD, 22 septembre 2015, disponible sur www.abc-bma.be/sites/default/files/content/download/files/2015pk27-aud-bma-pub.pdf.

144 Autorité de la concurrence, décision n° 17-D-06, 21 mars 2017, disponible sur www.autoritedelaconcurrence.fr/pdf/avis/17d06.pdf.

En vertu de cette « théorie des facilités essentielles », le refus, par une entreprise en position dominante sur un marché déterminé, de donner accès, à une autre entreprise, à une facilité – qui peut être un bien ou un droit de propriété intellectuel – dont elle est propriétaire (de droit ou « de fait ») constituera un abus de position dominante au sens de l'article 102 du TFUE si les « circonstances exceptionnelles » suivantes sont rencontrées : (i) l'accès à la facilité est indispensable pour permettre à l'entreprise requérant l'accès d'exercer ses activités sur un marché secondaire ; (ii) le refus élimine toute concurrence sur le marché secondaire ; (iii) le refus empêche l'apparition d'un nouveau produit ou service, ou d'innovations technologiques, qui ne sont pas offerts par l'entreprise en position dominante et pour lesquels il existe une demande potentielle des consommateurs ; et (iv) le refus ne peut être justifié par des considérations objectives[141].

40. Précisons toutefois que d'après l'autorité de la concurrence française et le Bundeskartellamt (l'autorité allemande de la concurrence), « ces conditions de la Cour de justice seront uniquement rencontrées s'il est démontré que les données de l'entreprise dominante sont véritablement uniques et qu'il n'existe pas d'autre possibilité pour le concurrent d'obtenir les données dont il a besoin pour offrir son service »[142].

À cet égard, il convient néanmoins de souligner que certaines données ont déjà été considérées comme étant indispensables, lorsque ces dernières ont été collectées dans le cadre d'anciens monopoles d'État. Ce fut notamment le cas en Belgique (affaire *Nationale Loterij*)[143] et en France (affaire *Engie*)[144].

41. Enfin, concluons notre propos relatif à l'interdiction des abus de position dominante en soulignant que, bien qu'étant un correctif relativement puissant, il sera rarement fait appel à l'article 102 du TFUE en pratique, car il permet uniquement de cibler un nombre limité d'entreprises, à savoir celles bénéficiant d'une position dominante sur un marché déterminé. Partant, de puissantes entreprises détentrices de données, qui ne bénéficieraient pas d'une telle position dominante, ne pourront être inquiétées sur cette base.

B. Législations sectorielles

42. Au titre des instruments juridiques limitant les droits sur les données, en favorisant leur circulation, les législations sectorielles occupent une place particulière. En effet, dès lors que les difficultés liées au contrôle et à l'accès aux données sont souvent propres à chaque secteur, une réponse ciblée peut s'avérer nécessaire. Dans cette contribution, nous nous cantonnerons à la présentation de trois de ces législations sectorielles, à savoir celles relatives aux secteurs automobile (1), bancaire (2) et public (3).

1. Secteur automobile

43. Le secteur automobile est probablement celui qui cristallise le plus les débats autour des questions de contrôle et d'accès aux données, et ce, notamment en raison du caractère toujours plus connecté de nos carrosses et de l'avènement prochain des véhicules autonomes.

44. La question de l'accès à certaines informations relatives au véhicule n'est toutefois pas nouvelle. Ainsi, dès 2007, un règlement européen relatif aux informations sur la réparation et l'entretien des véhicules fut adopté[145].

En vertu de ce règlement, les constructeurs automobiles ont l'obligation de fournir « un accès sans restriction et dans un format normalisé aux informations sur la réparation et l'entretien des véhicules aux opérateurs indépendants par l'intermédiaire de sites web, d'une manière aisément accessible et rapide, et qui soit non discriminatoire par rapport au contenu fourni et à l'accès accordé aux concessionnaires et aux réparateurs officiels »[146].

La *ratio legis* de ce texte est donc d'assurer une concurrence loyale entre les réparateurs indépendants et les concessionnaires et réparateurs officiels, en s'assurant qu'ils aient tous accès aux mêmes informations[147], et ce, à tout moment[148]. Dans le même ordre d'idées, les constructeurs doivent mettre des documents de formation à la disposition des opérateurs indépendants, comme ils le font pour les concessionnaires et les réparateurs officiels[149]. Le constructeur doit également mettre à disposition des réparateurs indépendants, sur son site web, les modifications ultérieures et les informations supplémentaires relatives à la réparation et l'entretien du véhicule concomitamment à la communication de ces éléments aux réparateurs officiels[150].

145 Règlement (CE) n° 715/2007 du Parlement européen et du Conseil du 20 juin 2007 relatif à la réception des véhicules à moteur au regard des émissions des véhicules particuliers et utilitaires légers (Euro 5 et Euro 6) et aux informations sur la réparation et l'entretien des véhicules, *J.O.*, L 171, 29 juin 2007.

146 Article 6, § 1er, du règlement n° 715/2007.

147 Les informations en cause sont listées à l'article 6, § 2, du règlement n° 715/2007.

148 Article 6, § 4, du règlement n° 715/2007.

149 Article 6, § 1er, du règlement n° 715/2007.

150 Article 6, § 7, alinéa 2, du règlement n° 715/2007.

Cet accès aux informations sur la réparation et l'entretien des véhicules n'est toutefois pas gratuit, dès lors que les constructeurs peuvent facturer des frais raisonnables et proportionnés[151]. Seront considérés comme déraisonnables ou disproportionnés les frais qui découragent l'accès en ne tenant pas compte de la mesure dans laquelle l'opérateur indépendant utilise les informations[152].

45. Plus récemment, les constructeurs automobiles se sont également vus invités à contribuer à la sécurité routière via l'établissement d'un cadre visant à soutenir le déploiement et l'utilisation coordonnés et cohérents de systèmes de transport intelligents (STI)[153] dans l'Union[154], notamment en vue de mettre en place un service d'appel d'urgence (eCall) interopérable dans toute l'Union[155], ainsi qu'une procédure pour la fourniture, dans la mesure du possible, d'informations minimales universelles sur la circulation, gratuites pour les usagers, liées à la sécurité routière[156]. Ces informations, ainsi que le contenu informationnel attendu, sont listées dans un règlement délégué de la Commission[157].

46. À l'heure actuelle, la question qui fait couler le plus d'encre dans le secteur automobile est celle de l'accès aux données des véhicules connectés et autonomes[158]. En effet, les réparateurs indépendants et autres développeurs de services, qui pourraient être éventuellement fournis aux passagers du véhicule autonome, craignent que les constructeurs automobiles ne leur refusent l'accès à certaines données clés, afin de favoriser les services que ces constructeurs offriraient eux-mêmes ou afin de favoriser les concessionnaires ou réparateurs officiels.

Ces crispations naissent du fait que, à ce jour, les constructeurs automobiles désirent opter pour le modèle du « véhicule étendu », en vertu duquel toutes les données produites par le véhicule sont transférées sur des serveurs externes propriétaires de ces constructeurs, conférant ainsi à ces derniers un contrôle exclusif (quasi monopolistique) sur ces données[159].

151 Article 7, § 1er, du règlement n° 715/2007.

152 *Ibid.*

153 « Système dans lequel des technologies de l'information et de la communication sont appliquées, dans le domaine du transport routier, y compris les infrastructures, les véhicules et les usagers, et dans la gestion de la circulation et la gestion de la mobilité, ainsi que pour les interfaces avec d'autres modes de transport » (article 4, § 1er, de la directive 2010/40/UE du Parlement européen et du Conseil du 7 juillet 2010 concernant le cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres modes de transport, *J.O.*, L 206, 6 août 2010).

154 Article 1er, § 1er, de la directive 2010/40.

155 Article 3, d), de la directive 2010/40.

156 Article 3, c), de la directive 2010/40.

157 Articles 3 et 4 du règlement délégué (UE) n° 886/2013 de la Commission du 15 mai 2013 complétant la directive 2010/40/UE du Parlement européen et du Conseil en ce qui concerne les données et procédures pour la fourniture, dans la mesure du possible, d'informations minimales universelles sur la circulation liées à la sécurité routière gratuites pour les usagers, *J.O.*, L 247, 18 septembre 2013.

158 Pour un article résumant et exposant la problématique, voy. W. Kerber, « Data Governance in Connected Cars : The Problem of Access to In-Vehicle Data », *JIPITEC*, 2018, pp. 310-331.

159 *Ibid.*, p. 311.

Les réparateurs et fournisseurs de services indépendants voient, dans cette position privilégiée des constructeurs, un risque de problème concurrentiel, et réclament dès lors des initiatives réglementaires relatives à l'accès à ces données, en vue d'assurer une concurrence juste et non faussée[160].

Plus précisément, ceux-ci réclament que le modèle du « véhicule étendu » soit abandonné au profit d'un modèle de « plateforme applicative à bord du véhicule »[161]. D'une part, ceci permettrait à ces réparateurs et fournisseurs de services indépendants d'avoir accès aux données directement sur le véhicule, en temps réel, plutôt que de devoir accéder aux données via un serveur externe contrôlé par les constructeurs, ce qui implique nécessairement un temps de latence[162]. D'autre part, cette solution permet de casser le monopole de fait des constructeurs sur ces informations, en confiant le contrôle de l'accès aux données du véhicule au propriétaire du véhicule, puisque le terminal de l'accès est situé à bord du véhicule, et non plus aux constructeurs, dans l'hypothèse où le terminal est un serveur externe au véhicule[163].

Les constructeurs automobiles, pour leur part, sont opposés à l'adoption d'un tel modèle de « plateforme applicative à bord du véhicule », pour des raisons de sécurité[164]. L'argument souvent avancé à cet égard est qu'en permettant l'accès aux données directement à bord du véhicule, plutôt que via un serveur externe, ceci crée des risques d'hacking du véhicule, et donc potentiellement des risques d'accidents. Cependant, un rapport rédigé par TRL[165], sur demande de la Commission, a démontré qu'une « plateforme applicative à bord du véhicule » pouvait être développée de façon telle qu'un niveau de sécurité élevé et adéquat soit assuré[166].

47. Bien que la Commission soit consciente de ces débats houleux, celle-ci a récemment indiqué qu'elle se limiterait, pour l'heure, à l'adoption d'une recommandation non contraignante en vue d'améliorer l'accès et la réutilisation des données des véhicules connectés et autonomes[167]. Celle-ci a toutefois indiqué qu'elle continuerait à superviser l'évolution de la situation et qu'elle se tiendrait prête à intervenir, le cas échéant, en vue d'établir un cadre plus contraignant pour le partage de données en vue d'assurer une concurrence loyale[168].

160 *Ibid.*
161 *Ibid.*
162 *Ibid.*, p. 314.
163 *Ibid.*, p. 311.
164 *Ibid.*
165 TRL, « Access to In-Vehicule Data and Resources – Final Report », 18 mai 2017, disponible sur https://ec.europa.eu/transport/sites/transport/files/2017-05-access-to-in-vehicle-data-and-resources.pdf.
166 *Ibid.*, p. 77 ; W. Kerber, « Data Governance in Connected Cars », *op. cit.*, p. 318.
167 Communication from the Commission to the European parliament, the Council, the European economic and social committee, the Committee of the Regions on the road to automated mobility : An EU strategy for mobility of the future, Bruxelles, 17 mai 2018, COM(2018) 283 final, p. 13.
168 *Ibid.*

2. *Secteur bancaire*

48. Un second secteur dans lequel les questions de contrôle et d'accès aux données ont récemment connu des remous est le secteur bancaire, en raison de l'adoption de la directive du 25 novembre 2015 concernant les services de paiement dans le marché intérieur[169] (dite « PSD2 »), transposée en droit belge par une loi du 19 juillet 2018 portant modification et insertion de dispositions en matière de services de paiement dans différents livres du Code de droit économique[170].

Cette réglementation permet ainsi aux prestataires de services d'initiation de paiement[171] et aux prestataires de services d'information sur les comptes[172] d'avoir accès aux données des comptes de paiement[173] des utilisateurs de leurs services[174]. Cet accès est toutefois assujetti au consentement explicite de l'utilisateur des services, à savoir le client[175].

L'objectif de cette réglementation est ainsi de permettre à des prestataires de services de paiement d'obtenir l'accès à certaines données des banques dans lesquelles les utilisateurs de ces services de paiement ont des comptes, afin de permettre la transaction[176].

Une telle réglementation vise notamment à éviter que les banques traditionnelles ne soient les seules à pouvoir mettre en place des services de paiement, en limitant leurs droits sur les données de comptes de paiement, par le biais d'une obligation d'octroi d'accès à des prestataires de services de paiement tiers.

49. Ainsi, grâce à la directive PSD2, un prestataire de services créant une application de paiement mobile (via smartphone), par exemple dénommée « Easypay », pourra obtenir l'accès aux données de compte en banque des utilisateurs de cette application, désirant effectuer une transaction, afin de s'assurer que celui-ci dispose des fonds suffisants et de valider la transaction.

169 Directive 2015/2366/UE du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE, *J.O.*, L 337, 23 décembre 2015.
170 Loi du 19 juillet 2018 portant modification et insertion de dispositions en matière de services de paiement dans différents livres du Code de droit économique, *M.B.*, 30 juillet 2018. Pour une contribution relative à l'impact, pour l'utilisateur, de cette loi de transposition, voy., dans cet ouvrage, C. Bourguignon, « L'utilisateur dans la nouvelle loi sur les services de paiement : entre protection et responsabilisation ».
171 « Service consistant à initier un ordre de paiement à la demande de l'utilisateur de services de paiement concernant un compte de paiement détenu auprès d'un autre prestataire de services de paiement » (article I.9, 33/11°, du Code de droit économique).
172 « Service en ligne consistant à fournir des informations consolidées concernant un ou plusieurs comptes de paiement détenus par l'utilisateur de services de paiement soit auprès d'un autre prestataire de services de paiement, soit auprès de plus d'un prestataire de services de paiement » (article I.9, 33/12°, du Code de droit économique).
173 « Compte qui est détenu au nom d'un ou de plusieurs utilisateurs de services de paiement et qui est utilisé aux fins de l'exécution d'opérations de paiement » (article I.9, 8°, du Code de droit économique).
174 Articles 66 et 67 de la directive 2015/2366 ; articles VII.35 et VII.36 du Code de droit économique.
175 Articles VII.35, § 2, et VII.63, alinéa 3, du Code de droit économique.
176 T. Thys, S. Van Raemdonck et K. Desmet, « GDPR, PSD2 and the Repurposing of Data : No Big Deal ? », *Droit bancaire et financier*, 2018, n° III, p. 185.

Cet accès ne pourra cependant se faire qu'à la condition que ce prestataire ait obtenu le consentement explicite de la part de l'utilisateur de l'application mobile[177]. En règle générale, ce consentement sera obtenu via l'adhésion aux conditions générales de l'application, dont l'utilisateur aura pris connaissance et qu'il aura acceptées préalablement au téléchargement de l'application sur son smartphone.

50. Enfin, précisons qu'un élément déterminant pour le fonctionnement de ce mécanisme d'accès aux données réside dans les modalités techniques mises en place pour permettre ledit accès.

De fait, tant la directive PSD2 que la loi de transposition sont muettes à cet égard. Chaque institution bancaire possédant ces données de compte de paiement est donc, *a priori*, libre de mettre en place le mécanisme d'accès qu'elle souhaite. Ceci risque néanmoins de générer des problèmes d'interopérabilité, si chacune de ces institutions développe un mécanisme sur base de standards techniques différents.

Ce faisant, il est intéressant de mentionner l'approche de la « UK Competition & Market Authority », qui requiert que les banques du Royaume-Uni mettent en place et assurent la maintenance d'une « interface de programmation applicative » (API)[178] commune et ouverte pour le secteur bancaire permettant, sur la base de standards techniques communs, aux prestataires de services de paiement répondant aux conditions de la directive PSD2 d'accéder aux données de ces banques[179]. Ceci permet en effet d'éviter les problèmes d'interopérabilité susmentionnés.

3. *Secteur public*[180]

51. Un dernier secteur méritant d'être mentionné est celui du secteur public. En effet, depuis quelques années, l'Union européenne se lance dans une démarche d'ouverture pour les données publiques, au bénéfice des citoyens et des entreprises.

a) Cadre légal relatif à la réutilisation des informations du secteur public

52. En 1999, la Commission européenne publie un livre vert intitulé « L'information émanant du secteur public : une ressource clef pour l'Europe »[181].

177 Articles VII.35, § 2, et VII.63, alinéa 3, du Code de droit économique.

178 « Le terme "interface de programme d'application" (API) désigne les interfaces d'applications ou les services web mis à disposition par les responsables du traitement de sorte que d'autres systèmes ou applications puissent se mettre en relation avec leurs systèmes et travailler avec ceux-ci » (Groupe 29, « Lignes directrices relatives au droit à la portabilité des données », *op. cit.*, p. 18).

179 UK Competition & Markets Authority, « Making Banks Work Harder for You », 9 août 2016, pp. 6-8, disponible sur www.agefi.fr/sites/agefi.fr/files/fichiers/2016/08/cma_overview-of-the-banking-retail-market_9_aout.pdf.

180 Pour une analyse plus détaillée, voy. M. KNOCKAERT, « La réutilisation des informations du secteur public : l'*open data* et les organismes publics », *J.T.*, 2018/27, n° 6739, pp. 613-621.

181 Commission européenne, « L'information émanant du secteur public : une ressource clef pour l'Europe. Livre vert sur l'information émanant du secteur public dans la société de l'information », COM(1998) 585, 20 janvier 1999.

Permettre et promouvoir la réutilisation des informations du secteur public bénéficie tant aux citoyens favorables à la transparence qu'aux administrations elles-mêmes, qui voient ainsi leur fonctionnement amélioré par l'échange d'informations et leurs interactions avec le monde extérieur. En outre, la réutilisation des informations publiques permet la croissance économique par le développement de nouveaux services et l'amélioration de la compétitivité entre les entreprises européennes, et entre ces dernières et les sociétés américaines. L'importance des données publiques ainsi démontrée, le texte dénonce l'absence d'un cadre réglementaire clair et prévisible au sein de l'Union.

53. La directive 2003/98/CE[182] est le premier texte communautaire d'harmonisation minimale en matière de réutilisation des informations du secteur public[183]. La directive précise que peuvent être réutilisables les documents existants détenus par les organismes du secteur public des États membres[184]. Le terme de document peut paraître inapproprié puisque l'essentiel pour le secteur économique est d'avoir accès à l'information dans sa substance même, au contenu, et de pouvoir en faire usage, sans considération de son enveloppe physique. Lors du processus d'adoption de la directive 2003/98/CE, le Parlement avait proposé de substituer à la notion de document celle d'information. Toutefois, il n'a pas été suivi sur ce point[185]. Pourtant, le titre de la directive met expressément l'information au cœur de la réglementation et le considérant 11 de la directive précise que le terme « document » recouvre une définition générique, qui tient compte de l'évolution de la société de l'information[186].

182 Directive 2003/98/CE du Parlement européen et du Conseil concernant la réutilisation des informations du secteur public, 17 novembre 2013, *J.O.*, L 345. La Belgique avait transposé fidèlement la directive. Au niveau fédéral, voy. la loi du 7 mars 2007 transposant la directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, *M.B.*, 19 avril 2007, p. 20982. Au niveau des entités fédérées : decreet van 27 april 2007 betreffende het hergebruik van overheidsinformatie, *M.B.*, 5 novembre 2007, p. 56250 ; ordonnance du 6 mars 2008 portant transposition de la directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, *M.B.*, 6 mars 2008, p. 18703 ; décret du 25 janvier 2007 portant transposition de la directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, *M.B.*, 19 février 2007, p. 7886 ; décret du 14 décembre 2006 portant transposition de la directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public et relatif à la publicité de l'administration dans les matières à l'égard desquelles la Région exerce les compétences de la Communauté française, *M.B.*, 28 décembre 2006, p. 74907 ; Dekret vom 18 Dezember 2006 über die Weiterverwendung öffentlicher Dokumente, *M.B.*, 15 mars 2007, p. 13831.

183 L. TERESI, *Droit de réutilisation et exploitation commerciale des données publiques*, Paris, La Documentation Française, 2011, pp. 33-46.

184 L'article 3 de la directive 2003/38/CE, dans sa première version, disposait que : « Les États membres veillent à ce que, lorsque la réutilisation de documents détenus par des organismes du secteur public est autorisée, ces documents puissent être réutilisés à des fins commerciales ou non commerciales conformément aux conditions définies aux chapitres III et IV. Si possible, les documents sont mis à la disposition du public sous forme électronique ».

185 L. TERESI, *Droit de réutilisation et exploitation commerciale des données publiques*, *op. cit.*, p. 115.

186 Considérant 11 de la directive 2003/98.

Dans sa première version, la directive n'emportait pas une réelle obligation des États membres à permettre la réutilisation des documents de leurs administrations[187]. Néanmoins, dans l'hypothèse où les services publics autorisaient la réutilisation des documents en leur possession, ils devaient le faire dans des conditions non discriminatoires, équitables et proportionnées[188]. En outre, les possibilités de réutilisation à des fins commerciales ou non ne pouvaient ni être indûment limitées ni avoir pour conséquence de restreindre la concurrence[189].

54. En 2013, dix ans après sa première publication, l'Union européenne modifie la directive sur la réutilisation des informations du secteur public. Ainsi, la directive 2013/37/UE du 26 juin 2013 concernant la réutilisation des informations du secteur public[190] marque un changement de paradigme fort en contraignant les autorités du secteur public à permettre à toute personne physique ou morale d'utiliser les documents qu'ils détiennent à des fins commerciales ou non commerciales. La seule limitation mise en place par le législateur européen se trouve dans la définition de la notion de réutilisation en indiquant qu'il doit s'agir d'une utilisation à des fins autres que l'objectif initial de la mission de service public pour lequel les documents ont été produits[191]. Les organismes du secteur public peuvent diffuser, notamment par le biais de leur site internet, les informations qu'ils détiennent et faciliter ainsi la circulation des données. À cela s'ajoute la possibilité pour quiconque d'adresser une demande de réutilisation à l'organisme concerné[192].

187 L'article 1er, § 3, de la directive 2003/98 dispose que : « La présente directive s'appuie sur les règles d'accès en vigueur dans les différents États membres et ne les affecte en rien. »

188 Considérant 8 de la directive 2003/98.

189 Article 8, § 1er, de la directive 2003/98.

190 Directive 2013/37/UE du Parlement européen et du Conseil modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public, 26 juin 2013, *J.O.*, L 175. Voy. également au niveau fédéral : loi du 4 mai 2016 relatif (*sic*) à la réutilisation des informations du secteur public, *M.B.*, 3 juin 2016, p. 34149. Au niveau des entités fédérées, voy. : decreet van 12 juni 2015 tot wijziging van het decreet van 27 april 2007 betreffende het hergebruik van overheidsinformatie en het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer, *M.B.*, 30 juin 2015, p. 37664 ; ordonnance du 27 octobre 2016 visant à l'établissement d'une politique de données ouvertes (Open Data) et portant transposition de la directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, *M.B.*, 10 novembre 2016, p. 74728 ; Dekret vom 29 juni 2015 zur Abänderung des Dekrets vom 18 Dezember 2006 über die Weiterverwendung öffentlicher Dokumente, *M.B.*, 17 juillet 2015, p. 46503 ; décret du 12 juillet 2017 relatif à la réutilisation des informations du secteur public et visant à l'établissement d'une politique de données ouvertes (« Open Data »), *M.B.*, 7 août 2017, p. 11932 ; décret conjoint du 12 juillet 2017 relatif à la réutilisation des informations du secteur public et visant à l'établissement d'une politique de données ouvertes (« Open Data ») pour les matières visées à l'article 138 de la Constitution, *M.B.*, 7 août 2017, p. 77945 ; décret conjoint de la Région wallonne et de la Communauté française du 19 juillet 2017 relatif à la réutilisation des informations du secteur public et visant à l'établissement d'une politique de données ouvertes (« Open Data »), *M.B.*, 13 septembre 2017, p. 83586.

191 Article 2, § 4, et considérant 8 de la directive 2003/98.

192 Article 4 de la directive 2003/98.

Ce principe est assorti de plusieurs exceptions, notamment pour respecter les règles nationales relatives à l'accès aux documents administratifs et pour maintenir l'intégrité des éventuels droits de propriété intellectuelle de tiers[193].

55. La directive a vocation à s'appliquer à l'ensemble du secteur public, que ce soit la filière politique, judiciaire ou administrative[194]. Elle s'applique aux organismes du secteur public et aux organismes de droit public. Ces expressions sont définies par référence à la réglementation relative aux marchés publics[195].

Par organismes du secteur public, sont visés l'État, les collectivités territoriales, les organismes de droit public et les associations formées par une ou plusieurs de ces collectivités ou un ou plusieurs de ces organismes de droit public.

Est également concerné tout organisme créé pour satisfaire spécifiquement des besoins d'intérêt général, ayant un caractère autre qu'industriel ou commercial. Toutefois, plusieurs conditions doivent être rencontrées afin que cet organisme entre dans le champ d'application de la directive. Premièrement, il doit être revêtu de la personnalité juridique. Deuxièmement, il est nécessaire que son activité soit majoritairement financée par l'État, les collectivités territoriales ou d'autres organismes de droit public ou que sa gestion soit soumise à un contrôle de ces derniers. Si la condition de financement ou de gestion n'est pas rencontrée, il faut alors que l'organe d'administration, de direction ou de surveillance de cet organisme soit composé de membres dont plus de la moitié sont désignés par l'État, les collectivités territoriales ou d'autres organismes de droit public[196].

En 2013, suite aux modifications apportées, la directive voit son champ d'application étendu au secteur culturel. Exclus initialement, les documents détenus par les bibliothèques, y compris les bibliothèques universitaires, les musées et archives sont dorénavant concernés par la réglementation relative à la réutilisation des informations du secteur public. Toutefois, en présence de droits de propriété intellectuelle détenus par l'institution culturelle elle-même, et contrairement aux organismes du secteur public, permettre la réutilisation n'est pas obligatoire[197].

56. Les considérations techniques sont une véritable nouveauté introduite en 2013 avec l'arrivée de nouvelles définitions telles que « format ouvert »[198], « format lisible par machine »[199] ou « norme formelle ouverte »[200]. L'on peut

193 Ces exceptions sont exhaustivement énumérées à l'article 1er, § 2, de la directive 2003/98 telle que modifiée par la directive 2013/37.

194 Considérant 16 de la directive 2003/98.

195 Considérant 10 de la directive 2003/98.

196 Article 2, 1), de la directive 2003/98.

197 Article 3, § 2, de la directive 2003/98 et considérants 14-19 de la directive 2013/37.

198 Article 2, § 7, de la directive 2003/98, inséré par la directive 2013/37.

199 Article 2, § 6, de la directive 2003/98, inséré par la directive 2013/37.

200 Article 2, § 8, de la directive 2003/98, inséré par la directive 2013/37.

déceler dans ces précisions le souci du législateur européen de faire de l'*open data* une politique commune au sein des différents États membres, en prévoyant une ouverture non pas uniquement juridique, mais également technique. La directive prévoit que les documents sont mis à disposition en vue d'une réutilisation dans un format lisible par machine[201]. Il revient donc aux administrations de diffuser ou délivrer les documents dans un format de fichier structuré de telle manière que des applications logicielles puissent identifier, reconnaître et extraire des données spécifiques[202]. En sus, le format lisible par machine doit être ouvert. Par cette exigence, il faut entendre que le format de fichier doit être indépendant des plateformes utilisées et mis à disposition du public sans restriction qui viendrait empêcher la réutilisation[203].

57. Si, depuis 2003, les organismes du secteur public ont le choix de diffuser purement et simplement leurs informations en affranchissant leur réutilisation de toutes conditions ou de la soumettre au respect de diverses conditions. À cet égard, la directive pose des balises. Les conditions posées par le secteur public ne peuvent ni indûment limiter les possibilités de réutilisation, ni avoir pour effet de restreindre la concurrence[204]. De plus, les conditions doivent être équitables, proportionnées et non discriminatoires[205]. Par conséquent, une politique de réutilisations différentes pour des catégories comparables de réutilisation ne peut pas être mise en place[206]. En tout état de cause, le nombre de restrictions imposées doit être le plus bas possible[207]. On observe que la directive mentionne expressément la possibilité pour les administrations d'imposer au réutilisateur de mentionner la source de l'information ou d'indiquer si le document a été modifié de quelque manière que ce soit[208].

58. En Belgique, une affaire particulièrement intéressante voit le jour en 2009[209]. L'affaire oppose la Banque-Carrefour des Entreprises (BCE) à Infobase Europe, société réutilisatrice des données de l'organisme public. Le conflit concerne certaines conditions de réutilisation contenues dans la licence élaborée par la BCE. Il s'agit de l'obligation pour le réutilisateur de céder ses propres données pour permettre à la BCE de corriger les siennes, de l'obligation d'accepter les audits de la BCE, de l'interdiction dans le chef d'Infobase de mettre les données de la BCE à disposition de tiers à titre gratuit et de l'interdiction de mettre les données de l'organisme public à disposition de tiers qui ne seraient pas des utilisateurs finals. La Cour d'appel rappelle que les organismes du secteur public ne disposent pas d'une liberté totale et que les conditions de réutilisation

201 Article 5, § 1er, de la directive 2003/98, tel que modifié par la directive 2013/37.
202 Voy. la définition énoncée à l'article 2, § 6, de la directive 2003/98, insérée par la directive 2013/37.
203 Voy. la définition énoncée à l'article 2, § 7, de la directive 2003/98, insérée par la directive 2013/37.
204 Article 8, § 1er, de la directive 2003/98.
205 Considérant 8 de la directive 2003/98.
206 Articles 8 et 10 de la directive 2003/98.
207 Considérant 26 de la directive 2013/37.
208 *Ibid.*
209 Bruxelles, 19 novembre 2009, *R.D.C.-T.B.H.*, 2009/8, pp. 835-844.

doivent être équitables, proportionnées et non discriminatoires. La Cour d'appel condamne la BCE pour sa première condition, à savoir l'obligation pour Infobase de céder ses propres données afin de corriger les informations de la BCE. Celle-ci est jugée disproportionnée. En effet, la correction des informations de la part d'Infobase constitue un investissement propre méritant une protection. La BCE utilise ainsi la licence pour profiter du travail fourni par le réutilisateur et faire siennes les données du réutilisateur à des fins d'exploitation[210].

59. Force est de constater que la directive sur la réutilisation des informations du secteur public vient amoindrir l'effet des droits de propriété intellectuelle détenus par les organismes du secteur public. En effet, le monopole conféré par un droit de propriété intellectuelle se trouve ainsi limité par l'obligation de permettre la réutilisation. De plus, la possibilité d'une rémunération est amoindrie depuis le changement introduit en 2013 concernant la tarification de la réutilisation, dorénavant limitée à une tarification à coût marginal (à l'exception notamment dans le cas des bibliothèques, musées et archives)[211].

b) Proposition de refonte de la directive 2013/37/UE

60. Le 25 avril 2018, la Commission européenne publie sa proposition de refonte de la directive sur la réutilisation des informations du secteur public[212] dans l'objectif de renforcer la position de l'Union dans une économie basée sur l'exploitation des données et de développer le marché intérieur. En substance, quatre modifications nous paraissent devoir être soulignées. Les principaux objectifs sont de renforcer l'*open data* au sein de l'Union européenne et de conférer une portée plus large au droit de réutilisation des informations du secteur public.

61. Premièrement, la Commission européenne souligne que les États membres confient souvent la prestation de services d'intérêt général à des entités en dehors du secteur public tout en maintenant un degré élevé de contrôle sur celles-ci[213]. Par conséquent, la proposition prévoit l'extension du champ d'application de la réglementation à certains documents détenus par certaines entreprises publiques. La notion d'entreprise publique est entendue comme « toute entreprise sur laquelle les organismes du secteur public peuvent exercer directement ou indirectement une influence dominante du fait de leur droit de propriété sur cette entreprise, de la participation financière qu'ils y détiennent ou des règles qui la régissent ». Ainsi, les entreprises exerçant des activités dans notamment les

210 *Ibid.*, pts 25-26.
211 Sur ce point, voy. également C. Ker, « Réutilisation des informations du secteur public : la transposition de la directive 2013/37/UE », *R.D.T.I.*, 2016, pp. 63-64.
212 Proposition de directive du Parlement européen et du Conseil concernant la réutilisation des informations du secteur public (refonte), 25 avril 2018, COM(2018) 234 final (ci-après « proposition de refonte de la directive »), disponible sur https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52018PC0234.
213 Considérant 20 de la proposition de directive.

domaines de l'eau, de l'énergie, des transports et des services postaux ou qui agissent en qualité d'opérateurs sont encouragées à permettre la réutilisation de leurs informations. La Commission précise que la directive n'emporte pas de réelle obligation à leur égard[214].

62. Deuxièmement, la réutilisation des informations s'appliquera également aux données de la recherche. La notion de « données de la recherche » est définie comme « des documents se présentant sous forme numérique, autres que des publications scientifiques, qui sont recueillis ou produits au cours d'activités de recherche scientifique et utilisés comme éléments probants dans le processus de recherche, ou dont la communauté scientifique admet communément qu'ils sont nécessaires pour valider des conclusions et résultats de la recherche »[215]. À cet égard, la recherche doit être financée par des fonds publics et l'accès à ces données doit être fourni par l'intermédiaire d'une archive ouverte institutionnelle ou thématique. De manière abstraite, la Commission précise qu'il doit être tenu compte des intérêts commerciaux légitimes et des droits de propriété intellectuelle préexistants[216]. La Commission précise également que la réutilisation de ces « données de la recherche » doit être gratuite[217].

63. Troisièmement, la réutilisation gratuite des ensembles de données de forte valeur est envisagée. Par « données de forte valeur », la Commission souhaite élargir son champ d'application aux « documents dont la réutilisation est associée à d'importantes retombées socioéconomiques, notamment parce qu'ils se prêtent à la création de services et d'applications à valeur ajoutée et en raison du nombre de bénéficiaires potentiels des services et applications à valeur ajoutée fondés sur ces ensembles de données »[218]. Une liste des données visées doit être élaborée par la Commission[219].

64. Quatrièmement, la proposition prévoit que les coûts liés à l'anonymisation des données à caractère personnel peuvent être imputés au réutilisateur[220]. Cette considération amène à une double réflexion. D'une part, il revient au responsable de traitement de s'assurer qu'une réelle anonymisation est possible. D'autre part, un coût trop élevé mis à charge du réutilisateur pourrait constituer un frein à la réutilisation, notamment pour certaines jeunes entreprises ou certains profils individuels, et desservir dès lors les objectifs poursuivis par l'Union européenne.

214 Articles 1er, § 1er, b), et § 2, b), 2, § 3, et 3, § 2, de la proposition de directive.

215 À titre d'exemple, sont visés des statistiques, des résultats d'expériences, des mesures, des observations faites sur le terrain, des résultats d'enquêtes, des enregistrements d'entretiens et des images, à l'exclusion des articles scientifiques présentant et commentant des résultats de recherche scientifique effectuée par les auteurs (considérant 23 de la proposition de directive).

216 Articles 1er, § 1er, c), 2, § 7, et 10 de la proposition de directive.

217 Article 6, § 5, de la proposition de directive.

218 Articles 2, § 8, 6, § 5, et 13 de la proposition de directive.

219 Article 13, § 1er, de la proposition de directive.

220 Articles 6, § 1er, § 3 et § 4, de la proposition de directive.

Section 2
Création d'une « économie européenne fondée sur les données »

65. Consciente de la valeur économique des données et de la nécessité de l'élaboration d'un cadre juridique clair en matière de régulation de celles-ci – comme nous l'avons exposé en guise d'introduction à la présente contribution –, la Commission affiche, depuis plusieurs années, la volonté de créer une « économie européenne fondée sur les données », ayant pour objectif de « créer un cadre juridique et politique clair et adapté [...], en supprimant les entraves qui s'opposent encore à la libre circulation des données et en dissipant l'insécurité juridique créée par les nouvelles technologies liées aux données »[221].

Pour ce faire, la Commission a, à l'origine, exploré la voie de la potentielle création d'un nouveau « droit du producteur de données », établissant une forme de propriété sur les données non personnelles[222], qui fut fortement critiquée[223] (§ 1). Ce faisant, la Commission a abandonné cette idée et s'est résolue à laisser au marché le soin de s'autoréguler, en se reposant sur le principe de la liberté contractuelle (§ 2).

Signalons ici que la Commission a également adopté, dans la perspective de la création d'une « économie européenne fondée sur les données », un règlement établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne[224], sur lequel nous ne nous attarderons toutefois pas dans cette contribution. En effet, l'objectif principal de ce règlement est d'interdire les exigences de localisation de données non personnelles, à moins que celles-ci ne soient justifiées par des motifs de sécurité publique dans le respect du principe de proportionnalité[225]. La volonté est ainsi de favoriser la circulation de données au sein du marché intérieur. Partant, ce règlement prévoit principalement des obligations pour les États membres et non pour les personnes physiques ou morales, à l'exception de la disposition relative à la portabilité des données non personnelles, qui a cependant déjà été commentée *supra*[226].

§ 1. Premier mouvement : vers la création d'un droit de propriété sur les données non personnelles ?

66. Comme indiqué ci-dessus, la Commission européenne a, à l'origine, exploré la voie de la potentielle création d'un nouveau « droit du producteur

221 Communication de la Commission, « Créer une économie européenne fondée sur les données », *op. cit.*, p. 5.

222 *Ibid.*, p. 15.

223 Voy. *infra*, point 72.

224 Règlement 2018/1807, *J.O.*, L 303, 28 novembre 2018.

225 Article 4 du règlement 2018/1807.

226 Voy. *supra*, point 37.

de données », établissant une forme de propriété sur les données non personnelles[227]. Selon la Commission, ceci aurait permis de clarifier la situation pour le producteur de données, tout en donnant aux utilisateurs la possibilité d'utiliser les données en question[228].

A. Droit du producteur de données

67. En vertu de ce droit, le producteur, défini comme étant le propriétaire ou l'utilisateur à long terme de la machine créant les données, se serait vu accorder un droit d'utiliser et d'autoriser l'utilisation de données à caractère non personnel[229]. L'élaboration d'un tel droit était cependant source d'incertitudes sur quatre plans, à savoir la nature du droit, le champ des données couvertes, l'attribution de la titularité du droit et la détermination d'exceptions au droit.

68. Concernant la nature du droit, la Commission envisageait deux options. La première était celle de la création d'un nouveau droit réel opposable *erga omnes*, conférant un droit exclusif d'utilisation de certaines données[230]. Dans une telle acception, ce droit aurait permis au titulaire de s'opposer à l'utilisation de certaines données par des tiers, indépendamment de toute relation contractuelle, et de réclamer le paiement de dommages et intérêts pour tout accès ou utilisation non autorisée des données[231]. Cependant, la Commission ne manquait pas de préciser qu'un tel droit n'aurait pas pu porter sur des données à caractère personnel, puisque le droit à la protection de ces dernières est un droit fondamental[232].

La seconde option était celle de la création d'une « série de droits purement défensifs », à l'instar de la protection accordée aux secrets d'affaires[233]. À l'inverse de l'approche plus protectrice de la première option, cette seconde option avait pour objectif d'accroître le partage de données, tout en rassurant les possesseurs de données en leur octroyant une série de droits en cas d'utilisation illicite des données par des tiers[234]. Comme le soulignait la Commission, « cette approche équivaut plutôt à la protection d'une "possession de fait" qu'à la protection d'une forme de "propriété" »[235]. S'il avait été opté pour une telle approche, se serait également posée la question de la nécessité de l'établissement d'une liste (limitative) d'hypothèses d'utilisation illicites[236].

227 Communication de la Commission, « Créer une économie européenne fondée sur les données », *op. cit.*, p. 15.
228 *Ibid.*
229 *Ibid.*
230 Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy Accompanying the Document « Communication – Building a European Data Economy », Bruxelles, 10 janvier 2017, SWD(2017) 2 final, p. 33.
231 *Ibid.*
232 *Ibid.* Sur cette question, voy. également *supra*, point 9.
233 *Ibid.* Concernant la protection des secrets d'affaires, voy. *supra*, points 29 à 32.
234 *Ibid.*, pp. 33-34.
235 *Ibid.*, p. 34. Traduction libre.
236 *Ibid.*

69. Concernant le champ d'application de ce droit, celui-ci se serait vraisemblablement limité aux données non personnelles ou anonymisées non encore structurées dans une base de données, ainsi qu'aux métadonnées[237] relatives à ces données[238]. Cependant, seul le niveau syntactique (les données et le code), et non le niveau sémantique de l'information ou des idées exprimées par ces données, aurait été protégé, afin d'éviter la création d'un « super droit de propriété intellectuelle »[239]. À titre d'exemple, ce droit n'aurait pas permis de protéger le rendu visuel d'une photographie numérique, par ailleurs protégé par le droit d'auteur, mais aurait conféré certains droits sur les données contenues dans ce fichier[240].

70. L'attribution de la titularité de ce droit aurait également été une question épineuse devant être solutionnée. Dans l'hypothèse dans laquelle l'option sélectionnée était celle de la création d'un droit réel, la Commission suggérait notamment d'attribuer le droit sur la base des investissements et des ressources consacrées à la création des données[241]. Concrètement, ceci aurait mené à l'attribution du droit au fabricant de la machine générant les données – celui-ci ayant investi dans cet outil – ou à l'opérateur économique utilisant cette machine[242]. Ceci n'aurait pas manqué de poser des difficultés d'attribution en pratique, d'autant plus que dans nombre de situations, plusieurs personnes ou entreprises investissent conjointement dans de telles machines, rendant l'identification précise d'un ou plusieurs titulaires virtuellement impossible[243].

En revanche, si l'option sélectionnée avait été celle de la création d'une série de droits purement défensifs, la Commission proposait d'attribuer ces droits aux « possesseurs de fait » légitimes de ces données, en assujettissant cependant cette protection à la condition que le possesseur de fait ait mis en place des mesures techniques de protection afin de limiter l'accès à ses données par des tiers[244].

71. Enfin, à l'instar des droits de propriété intellectuelle, il aurait également été requis de préciser une palette d'exceptions au droit. En pratique, ces exceptions se seraient matérialisées par l'obligation de partager les données dans certaines hypothèses[245].

Ainsi, si le droit avait été accordé à l'opérateur économique utilisant la machine, celui-ci aurait pu se voir imposer l'obligation de conférer, dans

237 « Une métadonnée ("donnée de/à propos de donnée") est une donnée servant à définir ou décrire une autre donnée quel que soit son support (papier ou électronique) » (https://fr.wikipedia.org/wiki/Métadonnée).
238 Commission Staff Working Document on the Free Flow of Data, *op. cit.*, p. 34.
239 *Ibid.*
240 *Ibid.*
241 *Ibid.*, pp. 34-35.
242 *Ibid.*, p. 35.
243 *Ibid.*
244 *Ibid.*
245 *Ibid.*

certains cas, l'accès aux données au fabricant de cette machine, et vice-versa[246]. Par ailleurs, une exception aurait pu être créée en vue de permettre l'accès, par les pouvoirs publics, aux données à des fins d'intérêt public (protection de l'environnement, amélioration de la mobilité, etc.)[247]. Enfin, la Commission proposait d'investiguer la piste d'une exception à des fins de recherche scientifique financée entièrement ou majoritairement par des fonds publics[248].

B. Critiques doctrinales

72. Si certains ont soutenu l'idée du développement d'un tel droit[249], force est de constater que de nombreux auteurs de doctrine ont, en revanche, fait part de leur inquiétude quant à la création d'un droit de « propriété » sur les données, en arguant qu'aucune justification économique ne permettait de soutenir une telle proposition[250]. En effet, il n'existe aucune preuve du fait que l'absence d'un tel droit engendre un manque d'incitant à la production, l'analyse ou la commercialisation de données[251], et la création d'un tel droit pourrait engendrer des juxtapositions disruptives et des problèmes de délimitations avec les droits de propriété intellectuelle existants[252].

De plus, comme le souligne W. Kerber, « la difficulté de la détermination du champ d'application d'un tel droit et de la personne à qui il devrait être attribué pourrait amener à un niveau significatif d'incertitude juridique ayant pour conséquence de générer des coûts élevés et des obstacles à l'innovation future »[253].

246 *Ibid.*

247 Communication de la Commission, « Créer une économie européenne fondée sur les données », *op. cit.*, p. 15.

248 Commission Staff Working Document on the Free Flow of Data, *op. cit.*, p. 36.

249 Voy. notamment B. Van Asbroeck, J. Debussche et J. César, « White Paper – Data Ownership in the Context of the European Data Economy : Proposal for a New Right », disponible sur www.twobirds.com/en/news/articles/2017/global/data-ownership-in-the-context-of-the-european-data-economy. Dans ce « White Paper », les auteurs proposent la création d'un droit de propriété non exclusif, flexible et extensible sur les données.

250 Voy., *inter alia*, J. Drexl, « Designing Competitive Markets for Industrial Data », *op. cit.*, pp. 30-38 ; A. Weibe, « Protection of industrial data – A new property right for the digital economy? », *Journal of Intellectual Property Law & Practice*, 2017, vol. 12, n° 1, pp. 66-71 ; B. Hugenholtz, « Data Property in the System of Intellectual Property Law : Welcome Guest or Misfit ? », *in* S. Lohsse, R. Schulze et D. Staudenmayer (dir.), *Trading Data in the Digital Economy : Legal Concepts and Tools*, Baden-Baden, Nomos, 2017, pp. 78-82 ; W. Kerber, « Governance of Data : Exclusive Property vs. Access », *IIC*, 2016, vol. 47, p. 761 ; W. Kerber, « Rights on Data : The EU Communication "Building a European Data Economy" from an Economic Perspective », *in* S. Lohsse, R. Schulze et D. Staudenmayer (dir.), *Trading Data in the Digital Economy : Legal Concepts and Tools*, Baden-Baden, Nomos, 2017, pp. 115-120 ; H. Zech, « Data as tradeable commodity », *in Idem*, pp. 51-79 ; A. Strowel, « Big Data and Data Appropriation in the EU », *in* T. Aplin (dir.), *Research Handbook on Intellectual Property and Digital Technologies*, Camberley, Edward Elgar, 2018 (à paraître).

251 J. Drexl, « Designing Competitive Markets for Industrial Data », *op. cit.*, pp. 30-34 ; A. Weibe, « Protection of industrial data », *op. cit.*, p. 67 ; B. Hugenholtz, « Data Property in the System of Intellectual Property Law », *op. cit.*, pp. 80-81 ; W. Kerber, « Governance of Data », *op. cit.*, p. 761 ; W. Kerber, « Rights on Data », *op. cit.*, pp. 115-120.

252 A. Weibe, « Protection of industrial data », *op. cit.*, pp. 67-68 ; B. Hugenholtz, « Data Property in the System of Intellectual Property Law », *op. cit.*, pp. 89-94.

253 W. Kerber, « Governance of Data », *op. cit.*, p. 761. Traduction libre.

Enfin, bien que le caractère non exclusif des données puisse être altéré par le biais de limitations contractuelles ou techniques, la référence au concept de « propriété » apparaît inappropriée au vu du caractère intangible et non rival[254] des données.

§ 2. Second mouvement : liberté contractuelle et autorégulation du marché

A. Liberté contractuelle et grands principes pour le partage de données entre entreprises

73. Compte tenu des critiques doctrinales brièvement décrites ci-dessus[255], la Commission européenne a, dès lors, abandonné l'idée de la création d'un « droit de propriété » sur les données. Néanmoins, à titre de solution de repli, celle-ci a établi, dans sa communication intitulée « Vers un espace européen commun des données », des grands principes pour le partage de données entre entreprises[256]. Ces principes sont toutefois non contraignants, en vue de respecter la liberté contractuelle des parties.

Premièrement, les accords contractuels doivent être transparents et compréhensibles quant aux données faisant l'objet de l'accord, quant aux personnes ayant accès aux données en question et quant aux finalités d'utilisation des données permises par le contrat[257]. Il convient en effet d'être précis sur la portée du contrat[258].

Deuxièmement, le contrat doit reconnaître que, dans l'hypothèse où de nouvelles données seraient générées suite à l'utilisation des données faisant l'objet de l'accord, l'ensemble des parties au contrat ont contribué à cette création commune de valeur[259]. Ce faisant, chacune des parties devrait se voir reconnaître un droit d'utilisation des nouvelles données créées, le cas échéant limité à certaines finalités.

Troisièmement, chaque partie se doit de respecter les intérêts commerciaux et les secrets d'affaires des autres parties[260]. Il est, de fait, évident que le contrat de partage de données ne peut servir de voie déguisée pour prendre connaissance des secrets d'affaires du cocontractant en vue de les divulguer.

254 Un bien est non rival si « [sa] consommation par une personne ne diminue pas la quantité de biens consomptibles par les autres – à savoir, de multiples personnes peuvent utiliser une information sans l'épuiser » (M.A. Carrier, « Limiting Copyright Through Property », *in* H.R. Howe et J. Griffiths (dir.), *Concepts of Property in Intellectual Property Law*, Cambridge, Cambridge University Press, 2013, p. 196).

255 Voy. *supra*, point 72.

256 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, « Vers un espace européen commun des données », Bruxelles, 25 avril 2018, COM(2018) 232 final, p. 12.

257 *Ibid.*

258 Pour plus de précisions sur le contenu du contrat, voy. *infra*, points 75 à 81.

259 Communication de la Commission, « Vers un espace européen commun des données », *op. cit.*, p. 12.

260 *Ibid.*

Partant, il est conseillé de prévoir une clause de non-divulgation dans les conventions en cause.

Quatrièmement, lorsque le contrat prévoit l'échange de données commercialement sensibles, cet accord doit également répondre à la nécessité de garantir une concurrence non faussée[261]. L'objectif ici est d'éviter qu'une entreprise ayant un pouvoir de négociation supérieur à celui de son cocontractant ne requière de ce dernier, comme condition de conclusion de l'accord, qu'il lui fournisse des données commercialement sensibles, qui seraient ensuite utilisées par cette entreprise pour concurrencer de manière faussée son cocontractant.

Cinquièmement, dans la mesure où de nouvelles données sont générées suite à l'utilisation des données faisant l'objet du contrat, celui-ci doit permettre la portabilité[262] des données « dans toute la mesure du possible »[263]. On veut ainsi éviter que l'une des parties ne soit « coincée »[264] dans cette relation contractuelle et ne puisse, à un moment donné, opter pour les services plus avantageux d'un autre prestataire, en raison de difficultés techniques liées à la récupération des données.

74. Bien que ces principes soient non contraignants, la Commission a indiqué qu'elle continuerait à évaluer si ceux-ci, accompagnés d'éventuels codes de conduite, s'avèrent suffisants pour maintenir des marchés ouverts et équitables, et que, si nécessaire, elle remédierait à la situation en prenant des mesures appropriées telles que des mesures sectorielles[265], à l'instar des mesures déjà adoptées dans les secteurs automobile et bancaire[266].

B. Recommandations quant aux stipulations contractuelles devant idéalement apparaître dans les contrats

75. En marge de la formulation des grands principes brièvement exposés ci-dessus[267], la Commission s'est également attelée à la formulation de recommandations plus concrètes quant aux stipulations contractuelles devant idéalement apparaître dans les contrats de partage de données[268], outre les clauses traditionnelles relatives à la durée du contrat et aux conditions de résiliation ou de résolution de celui-ci, les clauses de juridiction ou de droit applicable, etc.

261 *Ibid.*
262 Sur la portabilité des données à caractère personnel voy. *supra*, points 35 et 36. Sur la portabilité des données non personnelles, voy. *supra*, point 37.
263 Communication de la Commission, « Vers un espace européen commun des données », *op. cit.*, p. 12.
264 *Locked-in.*
265 Communication de la Commission, « Vers un espace européen commun des données », *op. cit.*, p. 12.
266 Voy. *supra*, points 43 à 50.
267 Voy. *supra*, points 73 et 74.
268 Commission européenne, Orientations concernant le partage des données du secteur privé dans l'économie européenne des données accompagnant la communication « Vers un espace européen commun des données », Bruxelles, 25 avril 2018, SWD(2018) 125 final, pp. 6-8.

76. Premièrement, il conviendra d'être aussi précis et concret que possible quant à la description des (jeux de) données faisant l'objet du contrat, ainsi que quant au rythme de mises à jour de ces données[269]. Il doit, en effet, être prévu si le partage sera réalisé par le biais d'un flux continu de données « en temps réel », ou, au contraire, par le biais de la transmission de blocs de données à intervalle régulier (tous les jours, semaines, mois...).

Il convient également de préciser le niveau de qualité et de fiabilité devant être atteint par ces données, ainsi que leur source et la manière dont elles ont été collectées[270]. Afin d'assurer que l'ensemble des parties contribuent à l'amélioration de la qualité de ces données, il est conseillé de mettre en place un mécanisme de notification des erreurs[271].

77. Deuxièmement, il est nécessaire de circonscrire les droits d'accès, de réutilisation et de distribution des données faisant l'objet du contrat, en définissant de façon transparente, claire et compréhensible les (catégories de) personnes pouvant poser ces actes, ainsi que les conditions auxquelles ces actes peuvent être posés[272].

Concernant le droit d'accès, celui-ci ne doit pas nécessairement être illimité, et il peut ainsi être restreint à certaines catégories de personnes physiques ou morales (chercheurs, ONG...) ou à certaines finalités déterminées[273].

Concernant la réutilisation et la distribution, il sera judicieux de préciser l'utilisation exacte qui peut être faite des données, ainsi que des données dérivées produites sur la base des analyses menées sur ces données primaires[274]. Par ailleurs, il conviendra d'être précis sur la possibilité, ou l'interdiction, pour le cocontractant d'octroyer des sous-licences, et, le cas échéant, de préciser les conditions dans lesquelles de telles sous-licences peuvent être octroyées[275]. Par exemple, le contrat pourrait prévoir que la conclusion d'une sous-licence est soumise à l'autorisation préalable du possesseur originaire des données.

78. Troisièmement, les moyens techniques concrets mis en place pour permettre l'accès et/ou le partage de données devraient être spécifiés dans le contrat, notamment en termes de fréquence et de volume, de niveau de services d'assistance et d'exigences de sécurité informatique[276]. Il conviendra ainsi notamment de prévoir si l'accès aux données se fait par le biais d'un transfert de données, ou par le biais d'une interface de programmation applicative,

269 *Ibid.*, p. 6.
270 *Ibid.*, p. 7.
271 *Ibid.*
272 *Ibid.*
273 *Ibid.*
274 *Ibid.*
275 *Ibid.*, p. 7.
276 *Ibid.*, pp. 7-8.

communément appelée « API »[277]. Concernant la sécurité, il est conseillé de prévoir dans le contrat que chacune des parties s'engage à garantir le caractère sécurisé de son infrastructure informatique, afin de mitiger au maximum les risques de fuite, de vol ou de destruction de données.

79. Quatrièmement, il conviendra bien évidemment d'inclure des clauses relatives à la responsabilité en cas de fourniture de données erronées ou de qualité médiocre, de perturbation dans la transmission de données, ou de destruction ou altération de données pouvant potentiellement engendrer un dommage[278]. À cet égard, il peut être intéressant de définir les droits pour chacune des parties d'effectuer des audits quant au respect de leurs obligations mutuelles[279].

80. Cinquièmement, il conviendra de prévoir le sort devant être réservé aux données ayant fait l'objet du contrat à l'issue de celui-ci. Pourraient ainsi être envisagées des obligations de restitution et/ou d'effacement, ou encore des limitations de finalités pour lesquelles ces données peuvent être utilisées à l'avenir par chacune des parties. Prévoir la restitution des données n'est, de fait, pas anodin, car, dans la grande majorité des cas, cette restitution ne pourra être imposée faute de stipulation contractuelle en ce sens. De même, il est suggéré de prévoir une telle obligation de restitution en cas de faillite du cocontractant.

81. Enfin, soulignons que la Commission a l'intention d'instituer un Centre de soutien pour le partage de données, ayant pour objectif de mettre en place une série de mesures destinées à faciliter le partage de données, notamment en fournissant des exemples de bonnes pratiques, des clauses contractuelles types ou des modèles de contrats existants[280].

C. Modèles de partage de données

82. Concluons cette seconde section en précisant que, si nous avons principalement envisagé, jusqu'à maintenant, l'hypothèse de contrats bilatéraux, il ne s'agit pas là de l'unique modèle de partage de données.

83. Ainsi, un second modèle de partage de données est celui des « places de marché de données »[281]. Dans ce modèle, un intermédiaire de confiance crée une plateforme permettant aux entreprises demandant ou offrant l'accès

277 « Le terme "interface de programme d'application" (API) désigne les interfaces d'applications ou les services web mis à disposition par les responsables du traitement de sorte que d'autres systèmes ou applications puissent se mettre en relation avec leurs systèmes et travailler avec ceux-ci » (Groupe 29, « Lignes directrices relatives au droit à la portabilité des données », *op. cit.*, p. 18).

278 Commission européenne, Orientations concernant le partage des données du secteur privé, *op. cit.*, p. 8.

279 *Ibid.*

280 *Ibid.*, p. 13.

281 Pour un exemple de place de marché de données, voy. www.dawex.com/fr/.

à des données de se rencontrer[282], à l'instar du fonctionnement d'une plateforme telle qu'eBay. Afin de rémunérer l'intermédiaire pour le service offert, celui-ci perçoit un pourcentage du montant de la transaction conclue sur sa plateforme[283].

84. Un troisième modèle de partage de données est celui des « plateformes de données industrielles ». À l'inverse du modèle précédent, la plateforme n'est pas ouverte à tous. En effet, dans ce modèle, un groupe restreint d'entreprises décide de s'unir afin de créer une plateforme sur laquelle celles-ci partagent, généralement gratuitement, certaines de leurs données dans un environnement fermé, exclusif et sécurisé[284].

La raison d'être de ces plateformes n'est donc pas la monétisation directe des données, mais plutôt l'amélioration des performances et des services de chaque entreprise, via l'obtention de l'accès à un plus grand nombre de données[285]. Citons, à titre d'exemple, la plateforme Skywise[286], créée par Airbus, sur laquelle cette dernière partage, avec les compagnies aériennes ayant acheté des avions Airbus pour leur flotte, toute une série de données relatives à ses avions[287].

Bien entendu, la constitution de telles plateformes doit se faire dans le respect de l'article 101 du TFUE[288] – interdisant les accords entre entreprises ayant pour objet ou pour effet d'empêcher, de restreindre ou de fausser la concurrence – et dans le respect de la législation relative à la protection des données.

85. Un quatrième modèle de partage de données, propre aux données à caractère personnel, est celui des systèmes de gestion d'informations personnelles (« PIMS »)[289], tels que MiData[290] au Royaume-Uni et MesInfos/SelfData[291] en France.

Concrètement, les personnes concernées ont recours à des services tiers de confiance, pouvant se présenter sous la forme de sites web, de plateformes, d'applications ou encore de « clouds » personnels, sur lesquels les responsables de traitements, qui ont accepté de participer au projet, partagent, avec le consentement de la personne concernée et au titre du droit à la portabilité[292], les données à caractère personnel de cette dernière qu'ils traitent[293]. Le fonc-

282 Everis, « Study on data sharing between companies in Europe », 2018, p. 62, disponible sur https://publications.europa.eu/en/publication-detail//publication/8b8776ff483411e8be1d01aa75ed71a1/language-en.

283 *Ibid.*

284 *Ibid.*

285 *Ibid.*

286 Voy. www.airbus.com/aircraft/support-services/skywise.html.

287 Everis, « Study on data sharing between companies in Europe », *op. cit.*

288 Traité sur le fonctionnement de l'Union européenne, *J.O.*, C-326/47, 26 octobre 2012.

289 *Personal information management systems* en anglais.

290 Voy. www.midata.coop/.

291 Voy. http://mesinfos.fing.org/selfdata/.

292 Voy. *supra*, points 35 et 36.

293 Voy. http://mesinfos.fing.org/selfdata/.

tionnement de ces PIMS est donc relativement semblable à celui des plateformes de données industrielles, si ce n'est qu'ici, la direction des opérations est conférée à la personne concernée, et non aux entreprises membres de la plateforme, dans un objectif de « data subject empowerment »[294].

86. Les quelques modèles décrits ci-dessus ne constituent naturellement pas une liste exhaustive. De fait, d'autres modèles, tels que le partage en accès libre de données[295] – calqué le cas échéant sur le régime de la directive PSI[296] – ou encore la fourniture de données en vue d'entraîner un algorithme, en l'échange d'un pourcentage du revenu qui sera ultérieurement généré par le service exploitant cet algorithme, peuvent être envisagés. Le principe de la liberté contractuelle permet, en effet, de laisser libre cours à l'imagination.

Conclusion

87. La détermination du cadre juridique applicable aux données est une tâche complexe, donnant ainsi la possibilité à de nombreuses personnes physiques ou morales de revendiquer un droit ou un intérêt à leurs traitements. Eu égard à la valeur économique évidente des données, à caractère personnel ou non, l'enjeu est pourtant crucial.

88. Cette contribution avait, ce faisant, un double objectif, dont le premier était de dresser un panorama du cadre juridique européen et belge actuel, applicable, directement ou indirectement, aux données.

D'une part, les instruments juridiques principaux conférant, potentiellement, des droits sur les données ont été présentés. Ont ici été envisagés les régimes de protection des données à caractère personnel, des secrets d'affaires, et de certains droits de propriété intellectuelle – à savoir le droit d'auteur et le régime *sui generis* de protection des bases de données – dans le cadre de l'analyse desquels les dispositions relatives au *text and data mining* ont également été étudiées.

D'autre part, certains instruments limitant les droits sur les données, en vue de favoriser leur circulation, ont été analysés. Dès lors qu'il n'était pas réaliste de s'atteler à la présentation de tous ces instruments, l'option fut prise de nous focaliser sur les deux instruments transversaux qui nous apparaissaient comme étant les plus pertinents – à savoir le droit à la portabilité des données et l'interdiction des abus de position dominante –, ainsi que sur les trois

294 Pour plus d'informations, voy. Th. Tombal, « Les droits de la personne concernée dans le RGPD », *op. cit.*, pp. 508-510.

295 Voy. notamment l'outil « Google Dataset Search » : https://toolbox.google.com/datasetsearch.

296 Voy. *supra*, points 51 à 64.

législations sectorielles que nous estimions être les plus abouties à ce stade – à savoir le secteur automobile, le secteur bancaire et le secteur public.

Le panorama ainsi dressé permet de mieux comprendre la complexité du cadre juridique potentiellement applicable aux données, d'autant que les divers instruments étudiés ne sont pas exclusifs les uns des autres, mais peuvent très bien, dans certains cas, s'appliquer cumulativement à un même jeu de données.

89. Le second objectif de cette contribution était de mettre en lumière les initiatives de la Commission européenne dans le cadre de la création d'une « économie européenne fondée sur les données ».

Pour ce faire, cette contribution a rappelé que, à l'origine, la Commission avait exploré la voie de la potentielle création d'un nouveau « droit du producteur de données », établissant une forme de propriété sur les données non personnelles, qui fut cependant fortement critiquée en doctrine. Ce faisant, la Commission a abandonné cette idée et s'est résolue à laisser au marché le soin de s'autoréguler, en se reposant sur le principe de la liberté contractuelle.

Néanmoins, à titre de solution de repli, celle-ci a établi, dans sa communication intitulée « Vers un espace européen commun des données », des grands principes, toutefois non contraignants, pour le partage de données entre entreprises. En marge de la formulation de ces grands principes, la Commission s'est également attelée à la formulation de recommandations plus concrètes quant aux stipulations contractuelles devant idéalement apparaître dans les contrats de partage de données, que nous avons ici détaillées.

Enfin, nous avons clôturé notre analyse par une présentation de divers modèles de partage de données.